Guia de Operações do OmniPGW

OmniPGW - Plano de Controle do Gateway de Pacote (PGW-C)

por Omnitouch Network Services

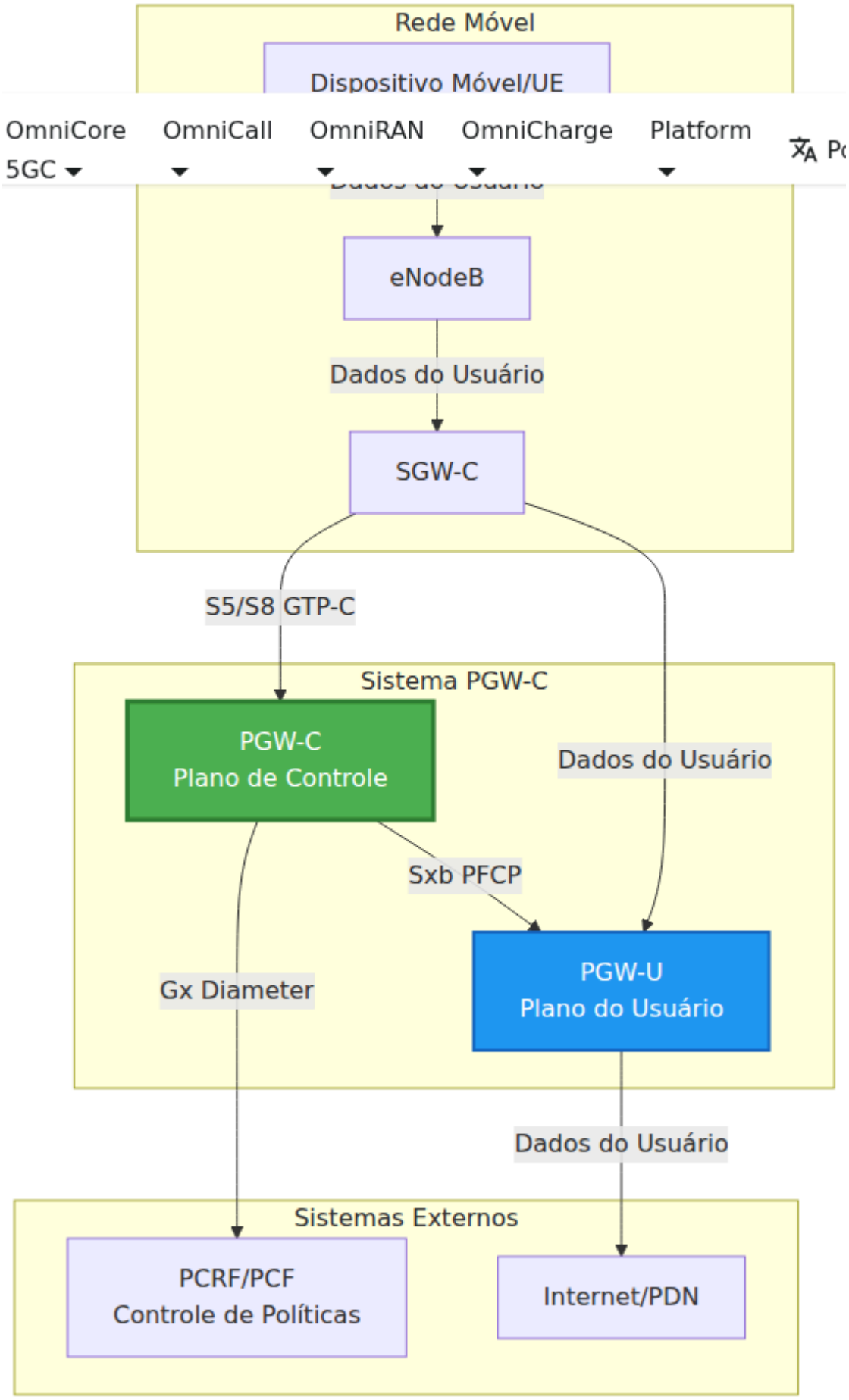
Índice

Visão Geral

OmniPGW é uma implementação de alto desempenho do Plano de Controle do Gateway de Pacote (PGW-C) para redes 3GPP LTE Evolved Packet Core (EPC), desenvolvida pela Omnitouch Network Services. Ele gerencia as funções do plano de controle para sessões de dados, incluindo:

- **Gerenciamento de Sessão** - Criar, modificar e encerrar sessões de dados do UE (Equipamento do Usuário)

- **Alocação de Endereço IP** - Atribuição de endereços IP a dispositivos móveis a partir de pools configurados
- **Controle de Políticas e Cobrança** - Interface com PCRF para aplicação de políticas e cobrança
- **Coordenação do Plano do Usuário** - Controle do PGW-U (Plano do Usuário) para encaminhamento de pacotes


Rede Móvel
Dispositivo Móvel/UE
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
eNodeB
Dados do Usuário
SGW-C
S5/S8 GTP-C
Sistema PGW-C
PGW-C
Plano de Controle
Dados do Usuário
Sxb PFCP
PGW-U
Plano do Usuário
Gx Diameter
Dados do Usuário
Sistemas Externos
PCRF/PCF
Controle de Políticas
Internet/PDN

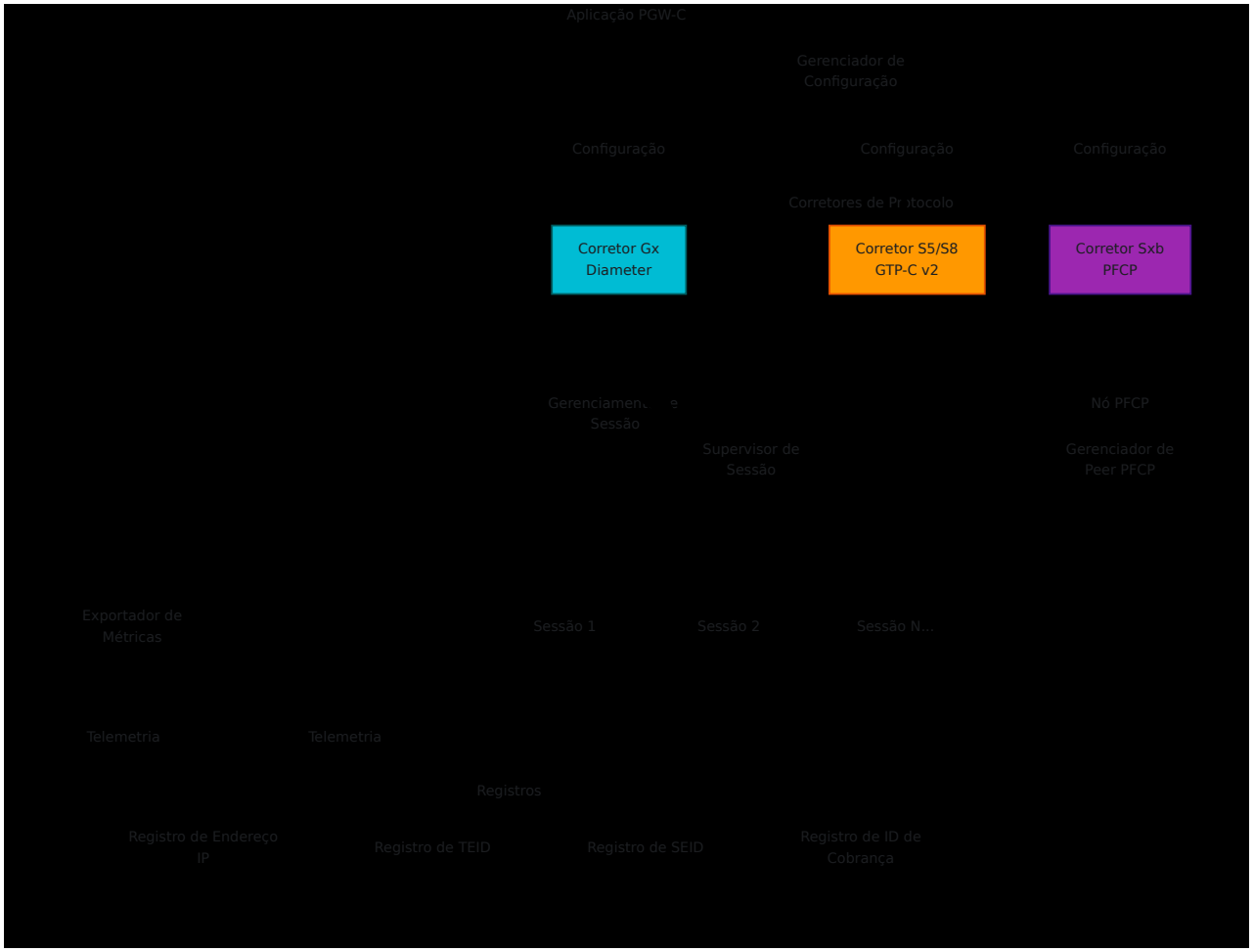
O que o PGW-C faz

- **Aceita solicitações de sessão** do SGW-C via interface S5/S8 (GTP-C)
- **Aloca endereços IP do UE** a partir de pools de sub-rede configurados
- **Solicita decisões de políticas** do PCRF via interface Gx (Diameter)
- **Programa regras de encaminhamento** no PGW-U via interface Sxb (PFCP)
- **Gerencia a aplicação de QoS** através de contextos de portadora e regras de QoS
- **Rastreia informações de cobrança** para sistemas de faturamento

---

Arquitetura

Visão Geral dos Componentes



Arquitetura do Processo

O PGW-C é construído sobre Elixir/OTP e utiliza uma arquitetura de processo supervisionada:

- **Supervisor da Aplicação** - Supervisor de nível superior que gerencia todos os componentes
- **Corretores de Protocolo** - Gerenciam mensagens de protocolo de entrada/saída
- **Processos de Sessão** - Um GenServer por conexão PDN ativa
- **Registros** - Rastreiam recursos alocados (IPs, TEIDs, SEIDs, etc.)
- **Gerenciador de Nó PFCP** - Mantém associações PFCP com peers PGW-U

Cada componente é supervisionado e será reiniciado automaticamente em caso de falha, garantindo a confiabilidade do sistema.

Interfaces de Rede

O PGW-C implementa três interfaces principais do 3GPP:

Interface S5/S8 (GTP-C v2)

Propósito: Sinalização do plano de controle entre SGW-C e PGW-C

Protocolo: GTP-C Versão 2 sobre UDP

Mensagens Chave:

- Solicitação/Resposta de Criação de Sessão
- Solicitação/Resposta de Exclusão de Sessão
- Solicitação/Resposta de Criação de Portadora
- Solicitação/Resposta de Exclusão de Portadora

Configuração: Veja Configuração S5/S8

Interface Sxb (PFCP)

Propósito: Sinalização do plano de controle entre PGW-C e PGW-U

Protocolo: PFCP (Protocolo de Controle de Encaminhamento de Pacotes) sobre UDP

Mensagens Chave:

- Solicitação/Resposta de Configuração de Associação
- Solicitação/Resposta de Estabelecimento de Sessão
- Solicitação/Resposta de Modificação de Sessão
- Solicitação/Resposta de Exclusão de Sessão
- Solicitação/Resposta de Heartbeat

Configuração: Veja Documentação da Interface PFCP/Sxb

Interface Gx (Diameter)

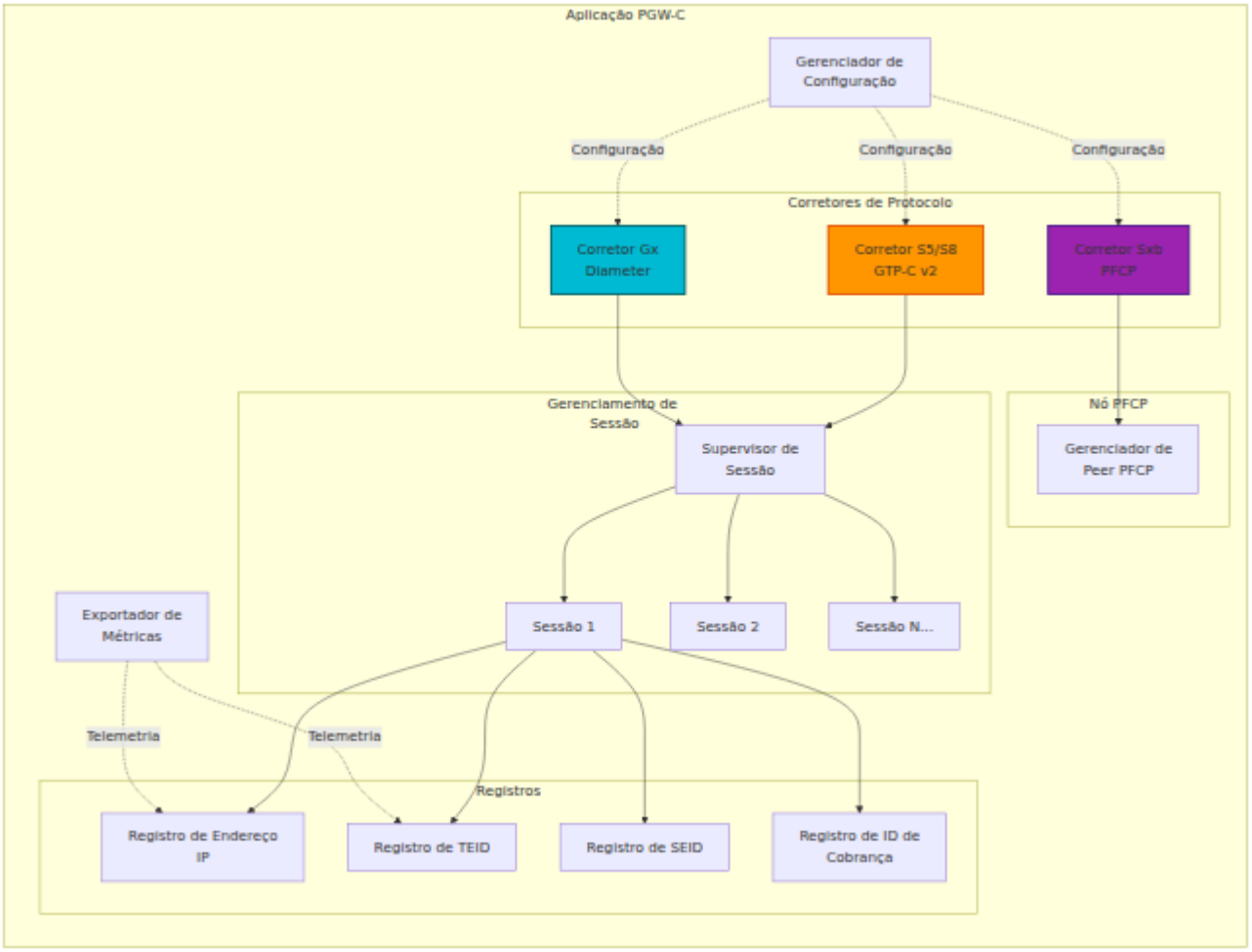
Propósito: Interface da Função de Regras de Políticas e Cobrança (PCRF)

Protocolo: Diameter (IETF RFC 6733)

Mensagens Chave:

- Solicitação/Resposta Inicial de Controle de Crédito (CCR-I/CCA-I)
- Solicitação/Resposta de Término de Controle de Crédito (CCR-T/CCA-T)

Configuração: Veja Documentação da Interface Diameter Gx



Conceitos Chave

Sessão PDN

Uma Sessão PDN (Rede de Dados de Pacote) representa a conexão de dados de um UE a uma rede externa (como a Internet). Cada sessão possui:

- **Endereço IP do UE** - Alocado a partir de um pool de sub-rede configurado
- **APN** (Nome do Ponto de Acesso) - Identifica a rede externa
- **Contexto de Portadora** - Contém parâmetros de QoS e informações de túnel
- **ID de Cobrança** - Identificador único para faturamento
- **TEID** (ID de Ponto de Extremidade do Túnel) - Identificador de túnel da interface S5/S8

- **SEID** (ID de Ponto de Extremidade da Sessão) - Identificador de sessão da interface Sxb

Contexto de Portadora

Uma portadora representa um fluxo de tráfego com características específicas de QoS:

- **Portadora Padrão** - Criada com cada sessão PDN
- **Portadoras Dedicadas** - Portadoras adicionais para necessidades específicas de QoS
- **EBI** (ID da Portadora EPS) - Identificador único para cada portadora
- **Parâmetros de QoS** - QCI, ARP, taxas de bits (MBR, GBR)

Regras PFCP

O PGW-C programa o PGW-U com regras de processamento de pacotes:

- **PDR** (Regra de Detecção de Pacotes) - Combina pacotes (uplink/downlink)
- **FAR** (Regra de A��ão de Encaminhamento) - Especifica o comportamento de encaminhamento
- **QER** (Regra de Aplicação de QoS) - Impõe limites de taxa de bits
- **BAR** (Regra de Ação de Bufferização) - Controla a bufferização de pacotes

Veja Documentação da Interface PFCP para detalhes.

Alocação de Endereço IP

Os endereços IP do UE são alocados a partir de pools de sub-rede configurados:

- **Seleção baseada em APN** - Diferentes APNs podem usar sub-redes diferentes
- **Alocação dinâmica** - Seleção aleatória de IP do intervalo disponível
- **Alocação estática** - Suporte para endereços IP solicitados pelo UE
- **Detecção de colisão** - Garante a atribuição única de IP

Veja Alocação de Pool de IP do UE para configuração.

Introdução

Pré-requisitos

- Elixir ~1.16
- Erlang/OTP 26+
- Conectividade de rede com SGW-C, PGW-U e PCRF
- Compreensão da arquitetura EPC LTE

Iniciando o OmniPGW

1. **Configure as configurações de tempo de execução** em `config/runtime.exs`
2. **Compile a aplicação:**

```
mix deps.get
mix compile
```

3. **Inicie a aplicação:**

```
mix run --no-halt
```

Verificando a Operação

Verifique os logs para um início bem-sucedido:

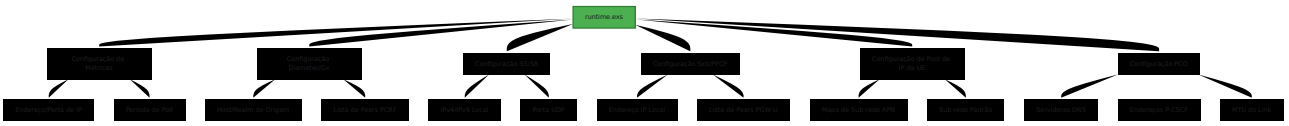
```
[info] Iniciando OmniPGW...
[info] Iniciando Exportador de Métricas em 127.0.0.42:42069
[info] Iniciando Corretor S5/S8 em 127.0.0.10
[info] Iniciando Corretor Sxb em 127.0.0.20
[info] Iniciando Corretor Gx
[info] Iniciando Gerenciador de Nó PFCP
[info] OmniPGW iniciado com sucesso
```

Acesse métricas em `http://127.0.0.42:42069/metrics` (endereço configurado).

Configuração

Toda a configuração em tempo de execução é definida em `config/runtime.exs`. A configuração é estruturada em várias seções:

Visão Geral da Configuração



Referência Rápida de Configuração

Seção	Propósito	Documentação
metrics	Exportador de métricas Prometheus	Guia de Monitoramento
diameter	Interface Gx para PCRF	Configuração Diameter Gx
s5s8	Interface GTP-C para SGW-C	Configuração S5/S8
sxb	Interface PFCP para PGW-U	Configuração PFCP
ue	Pools de endereços IP do UE	Configuração de Pool de IP
pco	Opções de Configuração de Protocolo	Configuração PCO
CDR	Cobrança offline & relatório de uso	Formato CDR

Veja o Guia Completo de Configuração para informações detalhadas.

Web UI - Painel de Operações em Tempo Real

O OmniPGW inclui uma **Web UI** integrada para monitoramento e operações em tempo real, fornecendo visibilidade instantânea sobre o status do sistema sem a necessidade de ferramentas de linha de comando ou consultas de métricas.

Acessando a Web UI

```
http://<omnipgw-ip>:<web-port>/
```

Páginas Disponíveis:

Página	URL	Propósito	Taxa de Atualização
Pesquisa de UE	`/ue_search`	Análise detalhada de sessões de assinantes específicas	Sob demanda
Sessões PGW	`/pgw_sessions`	Visualizar todas as sessões PDN ativas	2 segundos
Histórico de Sessões	`/session_history`	Log de auditoria de eventos de sessão	5 segundos
Topologia da Rede	`/topology`	Visualização da topologia da rede	5 segundos
Pools de IP	`/ip_pools`	Utilização do pool de endereços IP do UE	2 segundos
Sessões PFCP	`/pfcp_sessions`	Visualizar sessões PFCP com PGW-U	2 segundos
Status do UPF	`/upf_status`	Monitorar associações de peers PFCP	2 segundos
Seleção do UPF	`/upf_selection`	Visualizar regras de seleção do	Estático

Página	URL	Propósito	Taxa de Atualização
		UPF & status do P-CSCF	
Peers Diameter	`/diameter`	Monitorar conectividade PCRF	1 segundo
Monitoramento P-CSCF	`/pcscf_monitor`	Status da descoberta de DNS do P-CSCF	5 segundos
Simulador Gy	`/gy_simulator`	Testar cobrança online Gy/Ro	Sob demanda
Torres de Celular	`/cell_towers`	Navegar no banco de dados OpenCellID	Estático
Logs	`/logs`	Streaming de logs em tempo real	Ao vivo

Principais Recursos

Atualizações em Tempo Real:

- Todas as páginas atualizam automaticamente (sem necessidade de recarregar manualmente)
- Streaming de dados ao vivo dos processos do OmniPGW
- Indicadores de status codificados por cores (verde/vermelho)

Pesquisa & Filtro:

- Pesquisar sessões por IMSI, IP, MSISDN ou APN

- Filtragem instantânea sem recarregar a página

Detalhes Expansíveis:

- Clique em qualquer linha para ver detalhes completos
- Inspecionar estado completo da sessão
- Visualizar configuração e capacidades do peer

Sem Autenticação Necessária (Uso Interno):

- Acesso direto da rede de gerenciamento
- Projetado para uso da equipe NOC/operações
- Vincular apenas ao IP de gerenciamento por segurança

Fluxos de Trabalho Operacionais

Solução de Problemas de Sessão (Análise Detalhada):

```
1. Usuário relata problema de conexão
2. Abra a página de Pesquisa de UE (/ue_search)
3. Pesquise por IMSI, MSISDN ou endereço IP
4. Revise os detalhes abrangentes da sessão:
   a) Sessões Ativas - Verifique se a sessão existe com os
parâmetros corretos
   b) Localização Atual - Verifique TAC, ID da Célula, localização
geográfica
   c) Informações da Portadora - Verifique portadoras padrão e
dedicadas
      - QCI, MBR/GBR, Nomes de Regras de Cobrança
      - Limites APN-AMBR
   d) Informações de Cobrança - ID da sessão Gy, status da cota
   e) Informações de Política - sessão Gx, regras PCC instaladas
   f) Eventos Recentes - histórico de sessão e mudanças de estado
5. Se a sessão não for encontrada → Verifique a página Diameter
para conectividade PCRF
6. Se houver problemas de localização → Verifique os dados da
torre de celular na seção Localização Atual
```

Pesquisa Rápida de Sessão:

```
1. Usuário relata problema
2. Abra a página de Sessões PGW (/pgw_sessions)
3. Pesquise por IMSI ou número de telefone
4. Verifique se a sessão existe com detalhes básicos:
   - Endereço IP do UE alocado
   - Parâmetros de QoS
   - Pontos de extremidade do túnel estabelecidos
5. Para análise detalhada → Clique na sessão para expandir ou use
a Pesquisa de UE
```

Verificação de Saúde do Sistema:

```
1. Abra a página de Status do UPF → Verifique se todos os peers
PGW-U estão "Associados"
2. Abra a página Diameter → Verifique se todos os peers PCRF estão
"Conectados"
3. Abra Sessões PGW → Verifique a contagem de sessões ativas em
comparação com a capacidade
```

Monitoramento de Capacidade:

- Dê uma olhada na contagem de Sessões PGW
- Compare com a capacidade licenciada/esperada
- Identifique horários de uso máximo
- Monitore a distribuição entre APNs

Web UI vs. Métricas

Use a Web UI para:

- Solução de problemas detalhada de assinantes (Pesquisa de UE)
- Detalhes e inspeção de estado de sessões individuais
- Status de peers em tempo real (PFCP, Diameter)
- Verificações rápidas de saúde em todas as interfaces
- Solução de problemas de usuários específicos por IMSI/MSISDN/IP
- Verificação de localização geográfica (integração com Torre de Celular)
- Análise de QoS da portadora (MBR, GBR, QCI)

- Inspeção de regras de política e cobrança
- Histórico de sessão e trilhas de auditoria
- Monitoramento da capacidade do pool de IP
- Verificação de configuração e regras

Use Métricas Prometheus para:

- Tendências históricas
- Alertas e notificações
- Gráficos de planejamento de capacidade
- Análise de desempenho
- Monitoramento a longo prazo

Melhor Prática: Use ambos juntos - Web UI para operações imediatas, Prometheus para tendências e alertas.

Monitoramento & Métricas

Além da Web UI, o OmniPGW expõe métricas compatíveis com Prometheus para monitoramento:

Métricas Disponíveis

- **Métricas de Sessão**
  - `teid_registry_count` - Sessões S5/S8 ativas
  - `seid_registry_count` - Sessões PFCP ativas
  - `session_id_registry_count` - Sessões Gx ativas
  - `address_registry_count` - Endereços IP do UE alocados
  - `charging_id_registry_count` - IDs de cobrança ativas
- **Métricas de Mensagens**
  - `s5s8_inbound_messages_total` - Mensagens GTP-C recebidas
  - `sxb_inbound_messages_total` - Mensagens PFCP recebidas

    - `gx_inbound_messages_total` - Mensagens Diameter recebidas
    - Distribuições de duração de manipulação de mensagens

- **Métricas de Erro**

    - `s5s8_inbound_errors_total` - Erros de protocolo S5/S8
    - `sxb_inbound_errors_total` - Erros de protocolo PFCP
    - `gx_inbound_errors_total` - Erros Diameter

Acessando Métricas

As métricas são expostas via HTTP no endpoint configurado:

```
curl http://127.0.0.42:42069/metrics
```

Veja Guia de Monitoramento & Métricas para configuração de painel e alertas.

Documentação Detalhada

Esta seção fornece uma visão abrangente de toda a documentação do OmniPGW. Os documentos estão organizados por tópico e caso de uso.

Estrutura da Documentação

```
Documentação OmniPGW
├── OPERATIONS.md (Este Guia)
│
└── docs/
    ├── Configuração & Configuração
    │   ├── configuration.md          Referência completa do
runtime.exs
    │   ├── ue-ip-allocation.md       Configuração do pool de IP
    │   └── pco-configuration.md      Configurações de DNS, P-
CSCF, MTU
    │
    ├── Interfaces de Rede
    │   ├── pfcp-interface.md         Sxb/PFCP (comunicação PGW-U)
    │   ├── diameter-gx.md            Gx (comunicação PCRF)
    │   ├── diameter-gy.md            Gy/Ro (comunicação OCS)
    │   └── s5s8-interface.md         S5/S8 (comunicação SGW-C)
    │
    └── Operações
        ├── session-management.md     Ciclo de vida da sessão PDN
        └── monitoring.md             Métricas Prometheus &
alertas
```

Documentação por Tópico

Introdução

Documento	Descrição	Propósito
OPERATIONS.md	Guia principal de operações (este documento)	Visão geral e início rápido

⚙ Configuração

Documento	Descrição	Linhas
configuration.md	Referência completa do runtime.exs	1.600+
ue-ip-allocation.md	Gerenciamento e alocação de pool de IP do UE	943
pco-configuration.md	Opções de Configuração de Protocolo (DNS, P-CSCF, MTU)	344

Interfaces de Rede

Documento	Descrição	Linhas
pfcp-interface.md	Interface PFCP/Sxb para PGW-U	1.355
diameter-gx.md	Interface Diameter Gx para PCRF (Controle de Políticas)	941
diameter-gy.md	Interface Diameter Gy/Ro para OCS (Cobrança Online)	1.100+
s5s8-interface.md	Interface GTP-C S5/S8 para SGW-C	456

Operações & Monitoramento

Documento	Descrição	Linhas
session-management.md	Ciclo de vida e operações da sessão PDN	435
monitoring.md	Métricas Prometheus, painéis Grafana, alertas	807
data-cdr-format.md	Formato de arquivo CDR, configuração URR, cobrança offline	847
qos-bearers.md	Gerenciamento de QoS e portadoras, controle de políticas	448
troubleshooting.md	Procedimentos de solução de problemas e questões comuns	687

Recursos Avançados

Documento	Descrição	Linhas
pcscf-monitoring.md	Descoberta e monitoramento de saúde do P-CSCF	894

Recursos da Documentação

Diagramas Mermaid

Todos os documentos incluem **gráficos Mermaid** para compreensão visual:

- Diagramas de arquitetura
- Diagramas de sequência (fluxos de mensagens)
- Máquinas de estado
- Topologia da rede

Exemplos Práticos

Cada documento inclui:

- Exemplos de configuração do mundo real
- Configurações prontas para copiar e colar
- Casos de uso comuns

🔧 Solução de Problemas

Cada documento de interface inclui:

- Problemas comuns e soluções
- Comandos de depuração
- Métricas para diagnóstico

🔗 Referências Cruzadas

Os documentos estão extensivamente interligados para fácil navegação.

Caminhos de Leitura

Para Operadores de Rede

1. OPERATIONS.md - Visão geral (este documento)
2. configuration.md - Configuração
3. monitoring.md - Monitoramento
4. session-management.md - Operações do dia a dia

Para Engenheiros de Rede

1. OPERATIONS.md - Visão geral da arquitetura (este documento)
2. pfcp-interface.md - Controle do plano do usuário
3. diameter-gx.md - Controle de políticas
4. diameter-gy.md - Cobrança online
5. s5s8-interface.md - Gerenciamento de sessão
6. ue-ip-allocation.md - Gerenciamento de IP

Para Configuração & Implantação

1. configuration.md - Referência completa
2. ue-ip-allocation.md - Pools de IP
3. pco-configuration.md - Parâmetros de rede
4. monitoring.md - Configurar monitoramento

Estatísticas do Documento

- **Total de Documentos:** 14
- **Total de Linhas:** ~10.900+
- **Tamanho Total:** ~265 KB
- **Diagramas Mermaid:** 75+
- **Exemplos de Código:** 150+

Conceitos Chave Abordados

Arquitetura

- □ Separação do plano de controle/plano do usuário
- □ Arquitetura OTP/Elixir
- □ Supervisão de processos
- □ Sessões baseadas em GenServer

Protocolos

- □ PFCP (Protocolo de Controle de Encaminhamento de Pacotes)
- □ GTP-C v2 (Protocolo de Tunelamento GPRS)
- □ Diameter (RFC 6733)

Interfaces 3GPP

- □ Sxb (PGW-C ↔ PGW-U)
- □ Gx (PGW-C ↔ PCRF)
- □ Gy/Ro (PGW-C ↔ OCS)
- □ S5/S8 (SGW-C ↔ PGW-C)

Operações

- □ Gerenciamento de sessão
- □ Estratégias de alocação de IP
- □ Aplicação de QoS
- □ Integração de cobrança
- □ Monitoramento & alertas

Recursos Adicionais

Especificações 3GPP

Especificação	Título
TS 29.274	GTP-C v2 (interface S5/S8)
TS 29.244	PFCP (interface Sxb)
TS 29.212	Interface Diameter Gx (Controle de Políticas)
TS 32.299	Aplicações de Cobrança Diameter (Gy/Ro)
TS 32.251	Cobrança do domínio de Pacotes
TS 23.401	Arquitetura EPC

Documentação Relacionada

- Arquivo de configuração: config/runtime.exs

Guia de Configuração do OmniPGW

Referência Completa para Configuração do runtime.exs

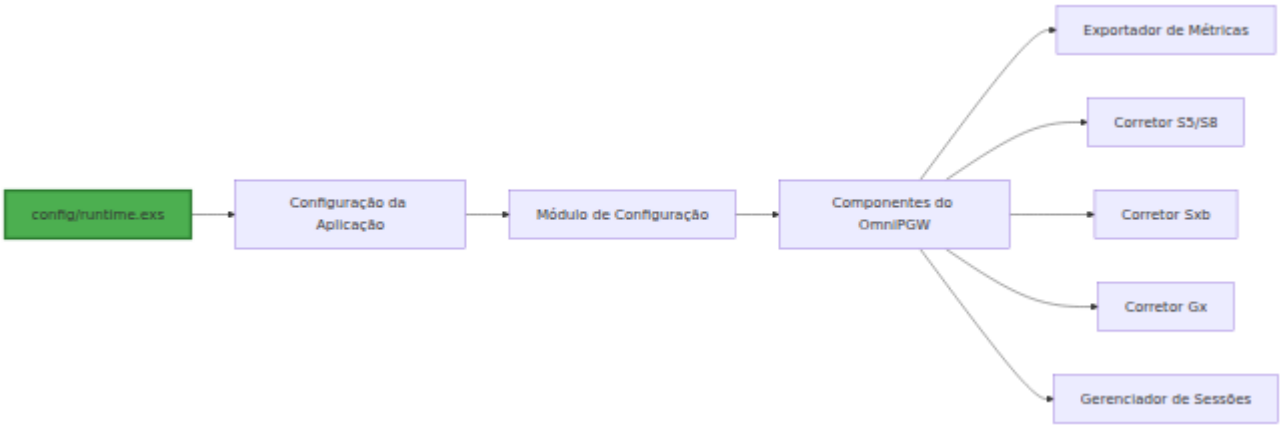
por Omnitouch Network Services

Índice

Visão Geral

OmniPGW utiliza **configuração em tempo de execução** definida em `config/runtime.exs`. Este arquivo é avaliado na **inicialização da aplicação** e permite configuração dinâmica com base em variáveis de ambiente ou fontes externas.

Filosofia de Configuração



Princípios Chave:

- **Fonte Única de Verdade** - Toda a configuração em um arquivo
- **Segurança de Tipo** - Configuração validada na inicialização
- **Flexibilidade de Ambiente** - Suporte para dev, teste, produção
- **Defaults Claros** - Defaults sensatos com substituições explícitas

---

Estrutura do Arquivo de Configuração

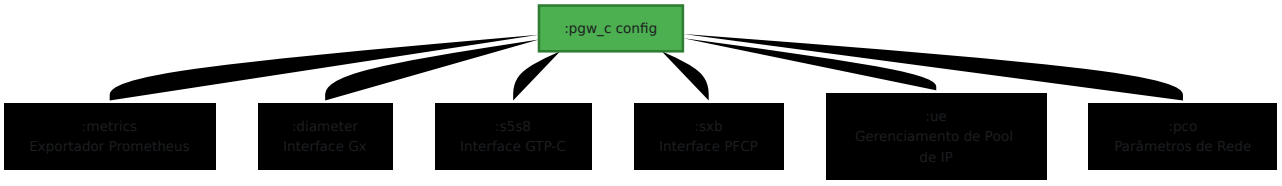
Localização do Arquivo

```
pgw_c/
├── config/
│   ├── config.exs         # Configuração base (importa
runtime.exs)
│   ├── dev.exs            # Configuração específica de
desenvolvimento
│   ├── prod.exs           # Configuração específica de produção
│   └── runtime.exs        # ← Arquivo de configuração principal
```

Estrutura de Nível Superior

```
# config/runtime.exs
import Config

config :logger, level: :info

config :pgw_c,
  metrics: %{...},
  diameter: %{...},
  s5s8: %{...},
  sxb: %{...},
  ue: %{...},
  pco: %{...}
```

Seções de Configuração



Configuração de Métricas

Propósito

Configurar o exportador de métricas Prometheus para monitorar o OmniPGW.

Bloco de Configuração

```
config :pgw_c,
  metrics: %{
    # Habilitar/desabilitar exportador de métricas
    enabled: true,

    # Endereço IP para vincular o servidor HTTP
    ip_address: "0.0.0.0",

    # Porta para o endpoint de métricas
    port: 9090,

    # Com que frequência consultar registros (milissegundos)
    registry_poll_period_ms: 10_000
  }
```

Parâmetros

Parâmetro	Tipo	Padrão	Descrição
`enabled`	Booleano	`true`	Habilitar exportador de métricas
`ip_address`	String (IP)	`"0.0.0.0"`	Endereço de vinculação (0.0.0.0 = todas as interfaces)
`port`	Inteiro	`9090`	Porta HTTP para o endpoint `/metrics`
`registry_poll_period_ms`	Inteiro	`10_000`	Intervalo de polling para contagens de registro

Exemplos

Produção - Vincular a um IP específico:

```
metrics: %{
  enabled: true,
  ip_address: "10.0.0.20",  # Rede de gerenciamento
  port: 9090,
  registry_poll_period_ms: 5_000  # Poll a cada 5 segundos
}
```

Desenvolvimento - Apenas localhost:

```
metrics: %{
  enabled: true,
  ip_address: "127.0.0.1",
  port: 42069,  # Porta não padrão
  registry_poll_period_ms: 10_000
}
```

Desabilitar métricas:

```
metrics: %{
  enabled: false
}
```

Acessando Métricas

```
# Endpoint padrão
curl http://<ip_address>:<port>/metrics

# Exemplo
curl http://10.0.0.20:9090/metrics
```

Veja: Guia de Monitoramento & Métricas para documentação detalhada sobre métricas.

Configuração do Diameter/Gx

Propósito

Configurar o protocolo Diameter para a interface Gx (comunicação PCRF).

Bloco de Configuração

```
config :pgw_c,
  diameter: %{
    # Endereço IP para escutar conexões Diameter
    listen_ip: "0.0.0.0",

    # Identidade Diameter do OmniPGW (Origin-Host)
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",

    # Reino Diameter do OmniPGW (Origin-Realm)
    realm: "epc.mnc001.mcc001.3gppnetwork.org",

    # Lista de pares PCRF
    peer_list: [
      %{
        # Identidade Diameter PCRF
        host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",

        # Reino PCRF
        realm: "epc.mnc001.mcc001.3gppnetwork.org",

        # Endereço IP PCRF
        ip: "10.0.0.30",

        # Iniciar conexão com PCRF
        initiate_connection: true
      }
    ]
  }
```

Parâmetros

Parâmetro	Tipo	Obrigatório	Descrição
`listen_ip`	String (IP)	Sim	Endereço de escuta do Diameter
`host`	String (FQDN)	Sim	Origin-Host do OmniPGW (deve ser FQDN)
`realm`	String (Domínio)	Sim	Origin-Realm do OmniPGW
`peer_list`	Lista	Sim	Configurações de pares PCRF

Configuração do Par:

Parâmetro	Tipo	Obrigatório	Descrição
`host`	String (FQDN)	Sim	Identidade Diameter do PCRF
`realm`	String (Domínio)	Sim	Reino do PCRF
`ip`	String (IP)	Sim	Endereço IP do PCRF
`initiate_connection`	Booleano	Sim	Se o OmniPGW conecta ao PCRF

Formato FQDN

Identidades Diameter DEVEM ser FQDNs:

```
# CORRETO
host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org"

# INCORRETO
host: "omnipgw"              # Não é um FQDN
host: "10.0.0.20"            # IP não permitido
```

Formato 3GPP:

```
<hostname>.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Exemplos:
- omnipgw.epc.mnc001.mcc001.3gppnetwork.org  (MCC=001, MNC=001)
- pgw-c.epc.mnc260.mcc310.3gppnetwork.org   (MCC=310, MNC=260 - T-Mobile dos EUA)
```

Exemplos

Um único PCRF:

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.0.30",
      initiate_connection: true
    }
  ]
}
```

Múltiplos PCRFs (Redundância):

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf-primary.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.1.30",
      initiate_connection: true
    },
    %{
      host: "pcrf-backup.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.2.30",
      initiate_connection: true
    }
  ]
}
```

Conexão Iniciada pelo PCRF:

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
  peer_list: [
    %{
      host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.0.0.30",
      initiate_connection: false  # Aguardar o PCRF conectar
    }
  ]
}
```

Veja: Documentação da Interface Diameter Gx

Configuração do S5/S8

Propósito

Configurar a interface GTP-C para comunicação com SGW-C.

Bloco de Configuração

```
config :pgw_c,
  s5s8: %{
    # Endereço IPv4 local para a interface S5/S8
    local_ipv4_address: "10.0.0.20",

    # Opcional: Endereço IPv6 local
    local_ipv6_address: nil,

    # Opcional: Substituir porta GTP-C padrão (2123)
    local_port: 2123,

    # Timeout de requisição GTP-C em milissegundos (padrão: 500ms)
    # Timeout por tentativa ao aguardar respostas GTP-C
    request_timeout_ms: 500,

    # Número de tentativas de reenvio para requisições GTP-C
(padrão: 3)
    # Tempo total máximo de espera = request_timeout_ms *
request_attempts
    request_attempts: 3
  }
```

Parâmetros

Parâmetro	Tipo	Padrão	Descrição
`local_ipv4_address`	String (IPv4)	Obrigatório	Endereço IPv4 da interface S5/S8
`local_ipv6_address`	String (IPv6)	`nil`	Endereço IPv6 da interface S5/S8 (opcional)
`local_port`	Inteiro	`2123`	Porta UDP para GTP-C (porta padrão 2123)
`request_timeout_ms`	Inteiro	`500`	Timeout por tentativa de reenvio em milissegundos
`request_attempts`	Inteiro	`3`	Número de tentativas de reenvio antes de desistir

Detalhes do Protocolo

- **Protocolo:** GTP-C Versão 2
- **Transporte:** UDP
- **Porta Padrão:** 2123
- **Direção:** Recebe de SGW-C

Exemplos

Apenas IPv4 (Comum):

```
s5s8: %{
  local_ipv4_address: "10.0.0.20"
}
```

IPv4 + IPv6 Dual-Stack:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  local_ipv6_address: "2001:db8::20"
}
```

Porta Personalizada (Não Padrão):

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  local_port: 2124  # Porta personalizada
}
```

Rede de Alta Latência:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  request_timeout_ms: 1500,  # 1.5 segundos por tentativa
  request_attempts: 3         # Total: 4.5 segundos no máximo
}
```

Configuração de Timeout

A interface S5/S8 utiliza timeouts configuráveis para transações de requisição/resposta GTP-C (Requisição de Criação de Bearer, Requisição de Exclusão de Bearer).

Cálculo do Tempo Total de Espera:

```
Tempo Máximo Total = request_timeout_ms × request_attempts
Padrão: 500ms × 3 = 1.5 segundos
```

Diretrizes de Ajuste:

Latência da Rede	Timeout Recomendado	Tempo Total de Espera
Baixa latência (<50ms)	200-300ms	600-900ms
Normal (50-150ms)	500ms (padrão)	1.5s
Alta latência (>150ms)	1000-2000ms	3-6s
Satélite/instável	2000-3000ms	6-9s

Quando Ajustar:

- **Aumentar timeout** se estiver vendo erros frequentes de "Requisição de Criação de Bearer expirou", mas o Wireshark mostra respostas chegando
- **Diminuir timeout** para detecção de falhas mais rápida em ambientes de baixa latência
- **Aumentar tentativas de reenvio** para redes não confiáveis com perda de pacotes

Comportamento de Timeout:

- No timeout, o erro é registrado: `"Requisição de Criação de Bearer expirou"`
- Erro Diameter retornado ao PCRF: Código de Resultado 5012 (UNABLE_TO_COMPLY)
- Bearer permanece em armazenamento inicial para limpeza quando a Regras de Cobrança-Remover chega

Planejamento de Rede

Seleção de Endereço IP:

- Use rede de gerenciamento/sinalização dedicada
- Garantir acessibilidade de todos os nós SGW-C

- Considerar redundância (VRRP/HSRP) para HA

Regras de Firewall:

```
# Permitir GTP-C do SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_c_network> -j ACCEPT
```

Configuração do Gn/Gp (GGSN)

Propósito

Configurar a interface GTP-C v1 para comunicação com SGSNs, habilitando a funcionalidade GGSN para redes 2G/3G.

Bloco de Configuração

```
config :pgw_c,
  gn: %{
    # Endereço IPv4 local para a interface Gn
    local_ipv4_address: "10.0.0.20",

    # Opcional: Endereço IPv6 local (a maioria das redes 2G/3G é
apenas IPv4)
    local_ipv6_address: nil,

    # Porta GTP-C (compartilhada com S5/S8)
    local_port: 2123
  },

  # Servidores DNS retornados no PCO (compartilhados com S5/S8)
  dns: %{
    primary_ipv4: {8, 8, 8, 8},
    secondary_ipv4: {8, 8, 4, 4}
  }
```

Parâmetros

Parâmetro	Tipo	Padrão	Descrição
`local_ipv4_address`	String (IPv4)	Obrigatório	Endereço IPv4 da interface Gn (endereço GGSN)
`local_ipv6_address`	String (IPv6)	`nil`	Endereço IPv6 da interface Gn (opcional, raramente usado)
`local_port`	Inteiro	`2123`	Porta UDP para GTP-C v1 (compartilhada com S5/S8)

Parâmetros DNS

Parâmetro	Tipo	Padrão	Descrição
`primary_ipv4`	Tupla	`{8, 8, 8, 8}`	Servidor DNS primário para resposta PCO
`secondary_ipv4`	Tupla	`{8, 8, 4, 4}`	Servidor DNS secundário para resposta PCO

Detalhes do Protocolo

- **Protocolo:** GTP-C Versão 1 (3GPP TS 29.060)
- **Transporte:** UDP
- **Porta Padrão:** 2123 (compartilhada com GTP-C v2)
- **Direção:** Recebe de SGSNs

Coexistência com S5/S8

OmniPGW pode operar como PGW (4G) e GGSN (2G/3G) simultaneamente:

- Ambas as interfaces compartilham a porta UDP 2123
- A versão GTP é detectada automaticamente a partir dos cabeçalhos de mensagem
- O mesmo endereço IP pode atender tanto ao tráfego 4G quanto ao 2G/3G
- Infraestrutura compartilhada: pools de IP, UPF/PFCP, cobrança online

Veja: Documentação da Interface Gn/Gp

Configuração do Sxb/PFCP

Propósito

Configurar a interface PFCP para comunicação com PGW-U (Plano do Usuário).

Bloco de Configuração

```
config :pgw_c,
  sxb: %{
    # Endereço IP local para comunicação PFCP
    local_ip_address: "10.0.0.20",

    # Opcional: Substituir porta PFCP padrão (8805)
    local_port: 8805
  }
```

Parâmetros

Parâmetro	Tipo	Padrão	Descrição
`local_ip_address`	String (IP)	Obrigatório	Endereço de escuta PFCP
`local_port`	Inteiro	`8805`	Porta UDP PFCP

> **Importante:**

> - **Todos os pares UPF são registrados automaticamente** a partir da configuração `upf_selection` (regras + pool de fallback) na inicialização
> - UPFs registrados automaticamente usam defaults sensatos:
>   - Nome gerado automaticamente: `"UPF-<ip>:<port>"`
>   - Associação PFCP passiva (aguarda o UPF iniciar)
>   - Intervalo de heartbeat de 5 segundos
> - Regras de seleção de UPF e pools são configurados na seção separada `upf_selection`. Veja Estratégias de Seleção de UPF abaixo.
> - Registro dinâmico de UPF é suportado para UPFs descobertos por DNS que não estão na configuração

Exemplos

Configuração Mínima:

```
sxb: %{
  local_ip_address: "10.0.0.20"
}

# Todos os UPFs em upf_selection serão registrados automaticamente
com:
# - Nome gerado automaticamente: "UPF-10.0.0.21:8805"
# - Associação PFCP passiva (aguarda o UPF conectar)
# - Intervalo de heartbeat de 5 segundos
```

Porta PFCP Personalizada:

```
sxb: %{
  local_ip_address: "10.0.0.20",
  local_port: 8806  # Porta PFCP não padrão
}
```

Exemplo Completo com Seleção de UPF:

```
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  rules: [
    %{
      name: "Pool IMS",
      priority: 10,
      match_field: :apn,
      match_regex: ~r/^ims$/,
      upf_pool: [
        %{remote_ip_address: "10.0.1.21", remote_port: 8805,
weight: 100},
        %{remote_ip_address: "10.0.1.22", remote_port: 8805,
weight: 100}
      ]
    }
  ],
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
100}
  ]
}
# Todos os 3 UPFs (10.0.1.21, 10.0.1.22, 10.0.2.21) são
registrados automaticamente
```

Seleção Baseada em DNS (Registro Dinâmico):

```
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai],
  dns_suffix: "epc.3gppnetwork.org",
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
100}
  ]
}
# UPFs descobertos por DNS serão registrados dinamicamente na
primeira utilização
```

Estratégias de Seleção de UPF

Importante: A configuração de seleção de UPF foi simplificada. Todos os pares UPF são registrados automaticamente a partir da configuração `upf_selection`.

Estrutura de Configuração

A seleção de UPF é configurada na seção **`upf_selection`** que define:

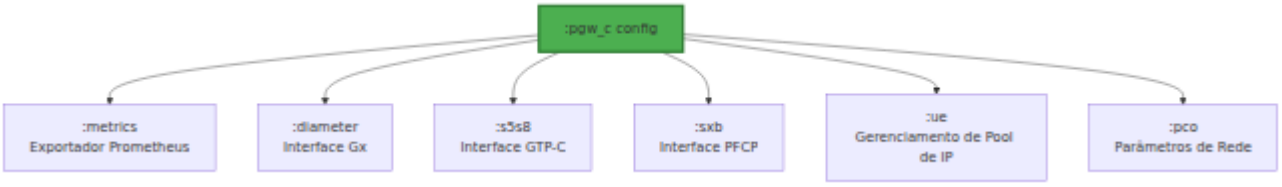
1. **Regras Estáticas** - Roteamento baseado em padrões com pools de balanceamento de carga
2. **Configurações de DNS** - Descoberta dinâmica de UPF baseada em localização
3. **Pool de Fallback** - Pool padrão quando nenhuma regra corresponde e DNS falha

Ordem de Prioridade da Seleção

1. **Regras Estáticas** (Maior Prioridade) - Roteamento baseado em padrões com pools de balanceamento de carga

2. **Seleção Baseada em DNS** (Menor Prioridade) - Descoberta dinâmica de UPF baseada em localização
3. **Pool de Fallback** (Menor Prioridade) - Pool padrão quando nenhuma regra corresponde e DNS falha

Fluxo de Decisão de Seleção de UPF



Campos de Correspondência Disponíveis

Regras estáticas podem corresponder a qualquer um desses atributos de sessão:

Campo de Correspondência	Descrição	Exemplo de Padrão
`:imsi`	Identidade Internacional de Assinante Móvel	`^313380.*` (operadora dos EUA)
`:apn`	Nome do Ponto de Acesso / DNN	`^internet\.` ou `^ims\.`
`:serving_network_plmn_id`	Identificador da rede servidora	`^313380$`
`:sgw_ip_address`	Endereço IP do SGW	`^10\.100\..*`
`:uli_tai_plmn_id`	ID PLMN da Área de Rastreamento	`^313.*`
`:uli_ecgi_plmn_id`	ID PLMN da Célula E-UTRAN	`^313.*`

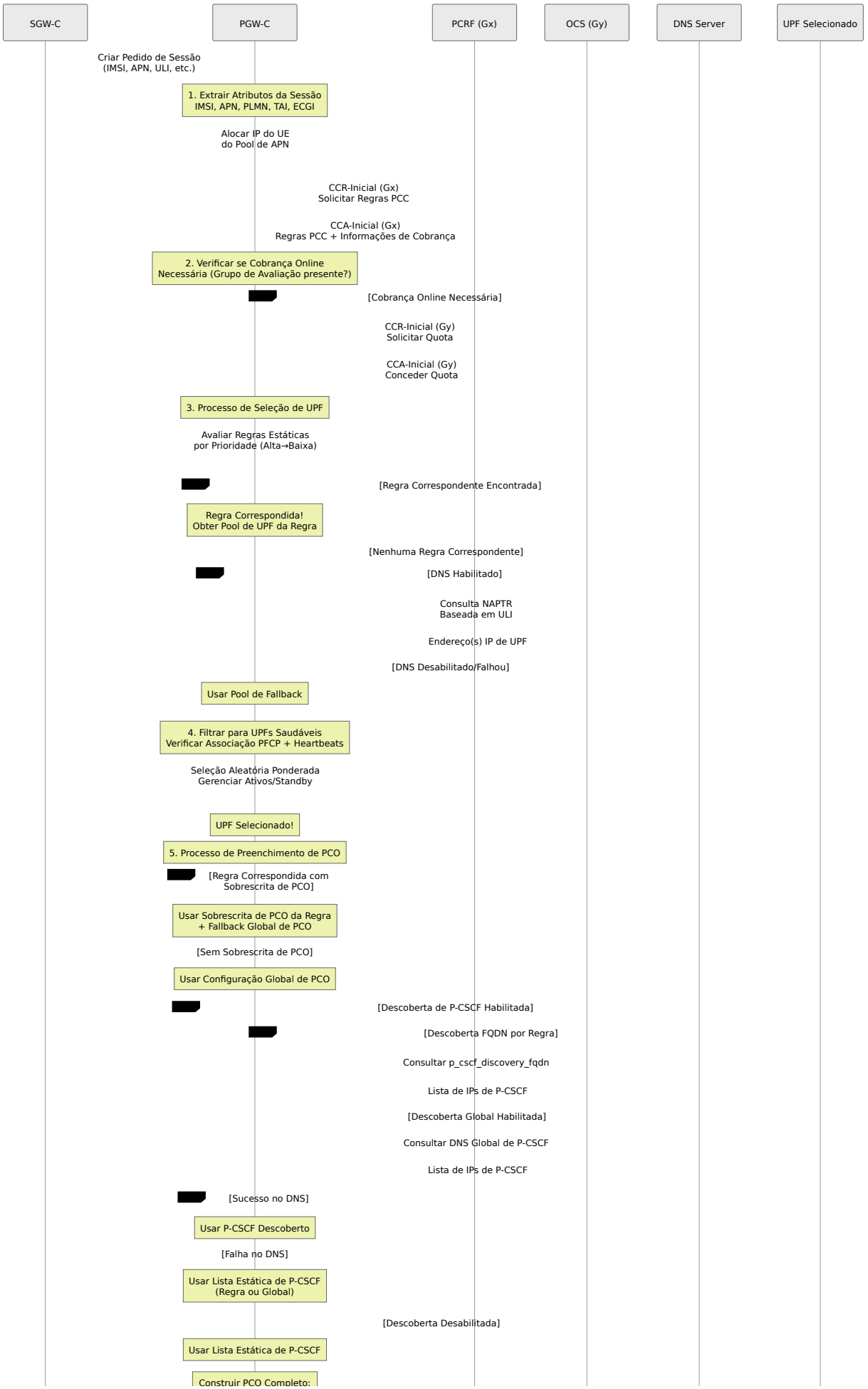
Comparação de Métodos de Seleção

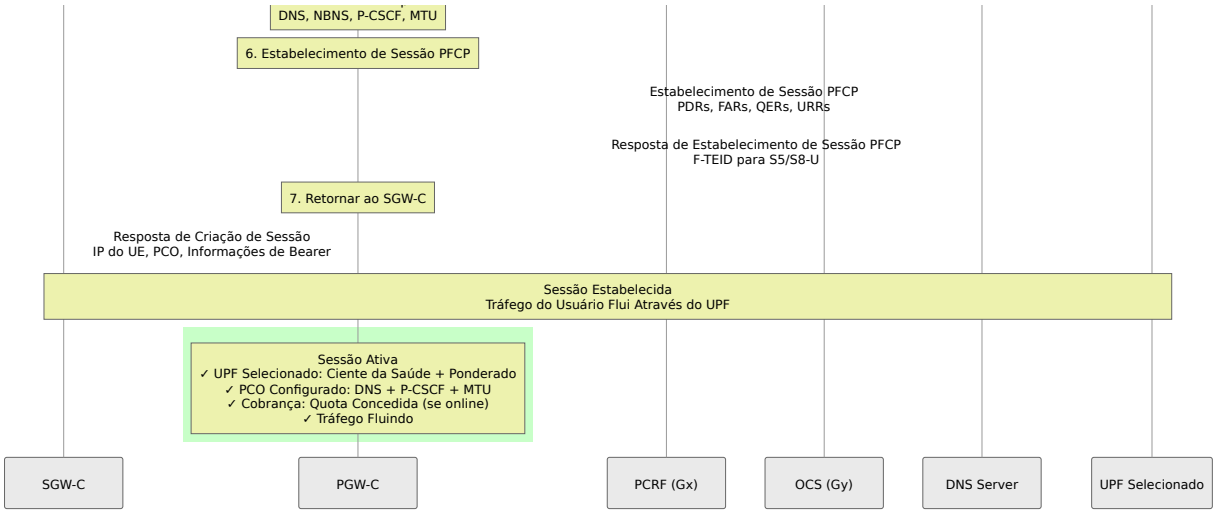
Método	Quando Usar	Prós	Contras
Pools de UPF	Implantações de produção	Balanceamento de carga, HA, pesos flexíveis	Requer múltiplos UPFs
Baseado em APN	Diferenciação de serviços	Roteia IMS/Internet separadamente	Configuração estática
Baseado em IMSI	Cenários de roaming	Roteamento geográfico	Complexidade de regex
Baseado em DNS	MEC/Computação de borda	Dinâmico, ciente da localização	Requer infraestrutura DNS
Pool de Fallback	Rede de segurança	Sempre ter um UPF	Pode não ser ótimo
Modo de Execução Simulada	Testando configs	Teste seguro	Sem tráfego real

---

Fluxo Completo de Estabelecimento de Sessão

Este diagrama mostra o fluxo completo de estabelecimento de sessão incluindo seleção de UPF e preenchimento de PCO:


SGW-C
PGW-C
PCRF (Gx)
OCS (Gy)
DNS Server
UPF Selecionado
Criar Pedido de Sessão (IMSI, APN, ULI, etc.)
1. Extrair Atributos da Sessão IMSI, APN, PLMN, TAI, ECGI
Alocar IP do UE do Pool de APN
CCR-Inicial (Gx) Solicitar Regras PCC
CCA-Inicial (Gx) Regras PCC + Informações de Cobrança
2. Verificar se Cobrança Online Necessária (Grupo de Avaliação presente?)
[Cobrança Online Necessária]
CCR-Inicial (Gy) Solicitar Quota
CCA-Inicial (Gy) Conceder Quota
3. Processo de Seleção de UPF
Avaliar Regras Estáticas por Prioridade (Alta→Baixa)
[Regra Correspondente Encontrada]
Regra Correspondida! Obter Pool de UPF da Regra
[Nenhuma Regra Correspondente]
[DNS Habilitado]
Consulta NAPTR Baseada em ULI
Endereço(s) IP de UPF
[DNS Desabilitado/Falhou]
Usar Pool de Fallback
4. Filtrar para UPFs Saudáveis Verificar Associação PFCP + Heartbeats
Seleção Aleatória Ponderada Gerenciar Ativos/Standby
UPF Selecionado!
5. Processo de Preenchimento de PCO
[Regra Correspondida com Sobrescrita de PCO]
Usar Sobrescrita de PCO da Regra + Fallback Global de PCO
[Sem Sobrescrita de PCO]
Usar Configuração Global de PCO
[Descoberta de P-CSCF Habilitada]
[Descoberta FQDN por Regra]
Consultar p_cscf_discovery_fqdn
Lista de IPs de P-CSCF
[Descoberta Global Habilitada]
Consultar DNS Global de P-CSCF
Lista de IPs de P-CSCF
[Sucesso no DNS]
Usar P-CSCF Descoberto
[Falha no DNS]
Usar Lista Estática de P-CSCF (Regra ou Global)
[Descoberta Desabilitada]
Usar Lista Estática de P-CSCF
Construir PCO Completo:



Pontos de Decisão Chave:

1. **Prioridade de Seleção de UPF:**
   - Regras Estáticas (Correspondência de Padrão) → Descoberta DNS → Pool de Fallback
   - Filtragem de saúde aplicada em todas as etapas
   - Lógica Ativa/Standby para alta disponibilidade
   - **Veja:** Interface PFCP para detalhes de comunicação UPF
2. **Prioridade de Preenchimento de PCO:**
   - Sobrescrita de PCO da Regra → Descoberta DNS de P-CSCF → Configuração Global de PCO
   - Mesclagem por campo (sobrescritas de regra substituem campos específicos, global fornece defaults)
   - **Veja:** Configuração de PCO para parâmetros detalhados de PCO
3. **Prioridade de Descoberta de P-CSCF:**
   - FQDN por Regra → Descoberta DNS Global → PCO Estático por Regra → PCO Estático Global
   - **Veja:** Monitoramento de P-CSCF para métricas de descoberta e rastreamento de saúde
4. **Integração de Cobrança:**
   - PCRF determina se a cobrança online é necessária (Grupo de Avaliação + Online=1)

- OCS concede quota antes do estabelecimento da sessão
- PGW-C rastreia quota e solicita mais via CCR-Update
- **Veja:** Interface Diameter Gx e Interface Diameter Gy para detalhes de cobrança

Exemplo Completo de Configuração

Aqui está um exemplo completo mostrando seleção de UPF com múltiplos pools e registro automático de pares:

```
config :pgw_c,
  # Interface PFCP - Todos os UPFs são registrados automaticamente
a partir de upf_selection
  sxb: %{
    local_ip_address: "127.0.0.20"
  },

  # Lógica de Seleção de UPF - Todos os UPFs definidos aqui são
registrados automaticamente
  upf_selection: %{
    # Configurações de seleção baseadas em DNS
    dns_enabled: false,
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
    dns_suffix: "epc.3gppnetwork.org",
    dns_timeout_ms: 5000,

    # Regras de seleção estáticas (avaliadas em ordem de
prioridade)
    rules: [
      # Regra 1: Tráfego IMS - Maior Prioridade
      %{
        name: "Tráfego IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
          %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
        ]
      },

      # Regra 2: APN Empresarial
      %{
        name: "Tráfego Empresarial",
        priority: 15,
        match_field: :apn,
        match_regex: "^(enterprise|corporate)\.apn",
        upf_pool: [
          %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
        ]
```

```
      },

      # Regra 3: Tráfego de Internet - Balanceado
      %{
        name: "Tráfego de Internet",
        priority: 5,
        match_field: :apn,
        match_regex: "^internet",
        upf_pool: [
          %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.22", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.23", remote_port: 8805,
weight: 34}
        ]
      }
    ],

    # Pool de fallback - Usado quando nenhuma regra corresponde e
DNS falha
    fallback_pool: [
      %{remote_ip_address: "127.0.0.21", remote_port: 8805,
weight: 100}
    ]
  }
```

Recursos Chave

Formato Atual:

- ✅ **Registro Automático**: Todos os UPFs de `upf_selection` são registrados automaticamente na inicialização
- ✅ **Configuração Centralizada**: Toda a seleção de UPF e configuração de pares em uma seção
- ✅ **Pools Necessários**: Todas as regras usam formato `upf_pool` (mesmo para um único UPF)
- ✅ **Fallback Estruturado**: Pool de fallback dedicado com distribuição ponderada
- ✅ **Integração DNS**: Configurações DNS ao lado das regras de seleção

- **Registro Dinâmico**: UPFs descobertos por DNS são registrados automaticamente na primeira utilização
- **Monitoramento de Saúde**: Todos os UPFs configurados são monitorados com heartbeats de 5 segundos

Migração do Formato Anterior:

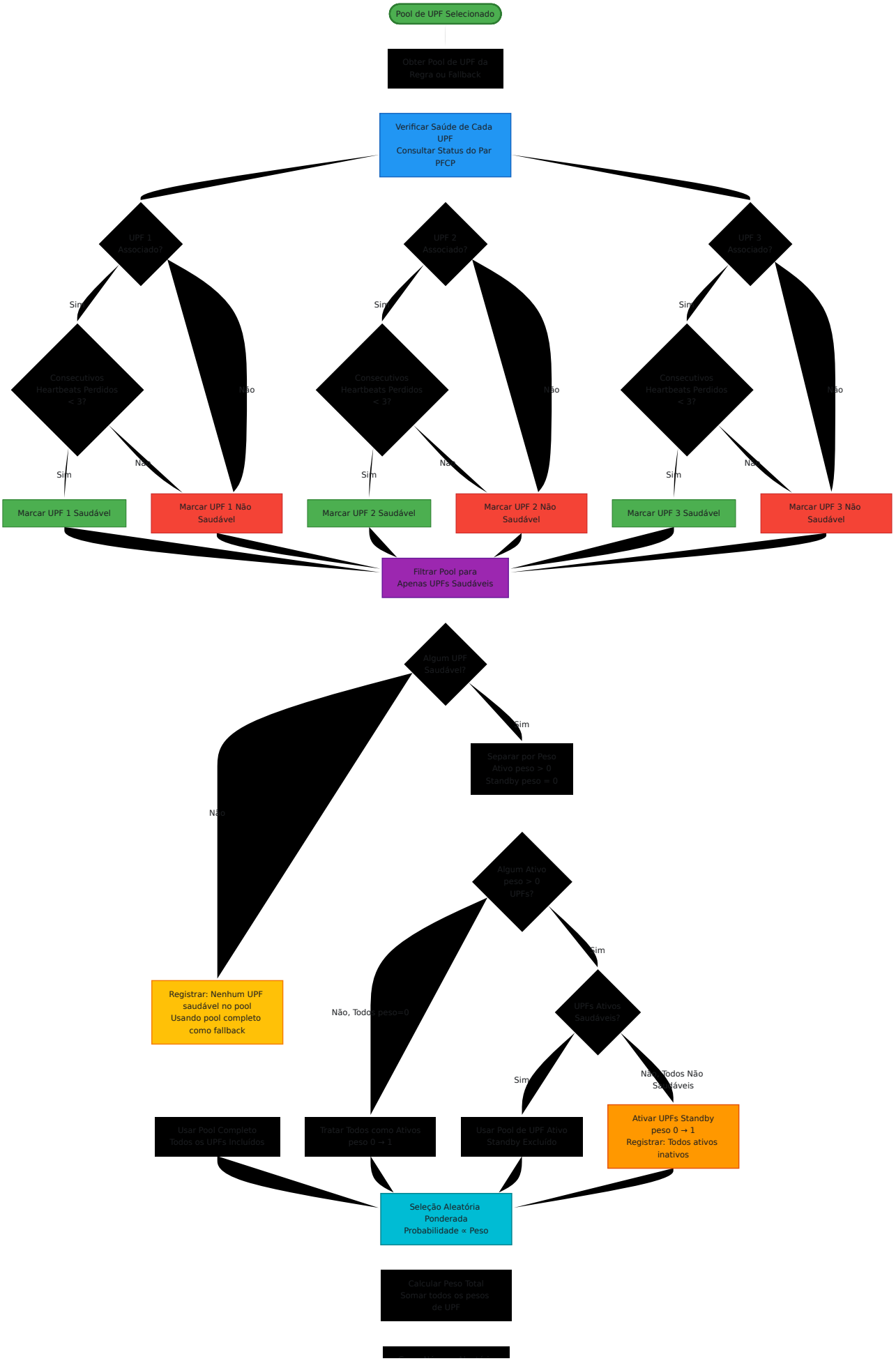
- Removido: campo `sxb.peer_list` (não é mais necessário)
- Removido: `selection_list` incorporado nas configurações de pares
- Todas as definições de UPF agora vão nas regras e pool de fallback de `upf_selection`

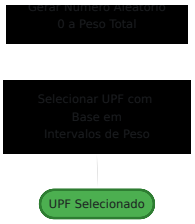
Como Funcionam os Pools de UPF:

1. **Seleção Ciente da Saúde**: Apenas UPFs saudáveis recebem tráfego
    - Saudável = associação PFCP ativa + menos de 3 heartbeats consecutivos perdidos
    - UPFs não saudáveis são automaticamente filtrados
    - Retorna a todos os UPFs se nenhum estiver saudável (falha rápida)
2. **Suporte Ativo/Standby**: Use `weight: 0` para UPFs de standby
    - **UPFs Ativos** (peso > 0): Recebem tráfego quando saudáveis
    - **UPFs Standby** (peso == 0): Recebem tráfego apenas quando todos os UPFs ativos estão inativos
    - UPFs de standby são tratados como `weight: 1` quando ativados
3. **Seleção Aleatória Ponderada**: Cada sessão é aleatoriamente atribuída a um UPF saudável com base nos pesos
    - No exemplo acima: 70% vão para .21, 20% para .22, 10% para .23
    - Peso maior = mais sessões atribuídas a esse UPF
    - Pesos iguais = distribuição igual
4. **Registro Automático**: Todos os UPFs nos pools são registrados automaticamente na inicialização
    - Nomes gerados automaticamente: `"UPF-<ip>:<port>"`

- Configurações padrão: associação PFCP passiva, heartbeats de 5 segundos
- Monitoramento de saúde imediato para todos os UPFs configurados

Seleção Ciente da Saúde com Ativo/Standby


Pool de UPF Selecionado
Obter Pool de UPF da Regra ou Fallback
Verificar Saúde de Cada UPF
Consultar Status do Par PFCP
UPF 1 Associado?
UPF 2 Associado?
UPF 3 Associado?
Sim
Não
Consecutivos Heartbeats Perdidos < 3?
Marcar UPF 1 Saudável
Marcar UPF 1 Não Saudável
Marcar UPF 2 Saudável
Marcar UPF 2 Não Saudável
Marcar UPF 3 Saudável
Marcar UPF 3 Não Saudável
Filtrar Pool para Apenas UPFs Saudáveis
Algum UPF Saudável?
Separar por Peso Ativo peso > 0 Standby peso = 0
Registrar: Nenhum UPF saudável no pool Usando pool completo como fallback
Algum Ativo peso > 0 UPFs?
UPFs Ativos Saudáveis?
Não, Todos peso=0
Todos Não Saudáveis
Usar Pool Completo Todos os UPFs Incluídos
Tratar Todos como Ativos peso 0 → 1
Usar Pool de UPF Ativo Standby Excluído
Ativar UPFs Standby peso 0 → 1 Registrar: Todos ativos inativos
Seleção Aleatória Ponderada Probabilidade ∝ Peso
Calcular Peso Total Somar todos os pesos de UPF



Exemplo de Seleção Aleatória Ponderada:

```
Pool: [
  UPF-A: peso 50, saudável ✓
  UPF-B: peso 30, saudável ✓
  UPF-C: peso 20, saudável ✓
]

Peso Total: 50 + 30 + 20 = 100

Intervalos de Peso:
  UPF-A: 0-49   (50%)
  UPF-B: 50-79  (30%)
  UPF-C: 80-99  (20%)

Número aleatório: 63 → Seleciona UPF-B
Número aleatório: 15 → Seleciona UPF-A
Número aleatório: 91 → Seleciona UPF-C
```

Exemplo de Failover Ativo/Standby:

```
Pool Inicial: [
  UPF-A: peso 100, saudável ✓   (Ativo)
  UPF-B: peso 0, saudável ✓     (Standby)
]

Cenário 1: UPF-A Saudável
→ Usar Pool Ativo: [UPF-A: 100]
→ Todo tráfego para UPF-A

Cenário 2: UPF-A Falha
→ Nenhum UPF ativo saudável
→ Ativar Standby: [UPF-B: 1]
→ Todo tráfego falha para UPF-B
→ Registrar: "Todos os UPFs ativos inativos, ativando UPFs
standby"

Cenário 3: Ambos Não Saudáveis
→ Nenhum UPF saudável
→ Usar pool completo: [UPF-A: 100, UPF-B: 0]
→ Selecionar com pesos (tentar conexão, pode falhar)
→ Registrar: "Nenhum UPF saudável no pool, usando pool completo
como fallback"
```

Padrões de Peso Comuns:

```
# Distribuição igual (25% cada)
upf_pool: [
  %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 1},
  %{remote_ip_address: "10.0.1.4", remote_port: 8805, weight: 1}
]

# Primário/backup balanceado (90% / 10%)
upf_pool: [
  %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
90},
  %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 10}
]

# Ativo/Standby (100% primário, 0% standby até primário falhar)
upf_pool: [
  %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
100},  # Ativo
  %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 0}
# Standby (apenas quando ativo falhar)
]

# Ativo com múltiplos standbys (balanceado quando ativado)
upf_pool: [
  %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight:
100},   # Ativo
  %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 0},
# Standby 1
  %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 0}
# Standby 2
]
# Resultado: Ativo recebe 100%. Se ativo falhar, standbys recebem
50/50%.

# Teste A/B (50% / 50%)
upf_pool: [
  %{remote_ip_address: "10.0.1.100", remote_port: 8805, weight:
50},  # Versão antiga
  %{remote_ip_address: "10.0.1.200", remote_port: 8805, weight:
50}   # Nova versão
]
```

Casos de Uso:

- **Failover Ativo/Standby**: Use `weight: 0` para UPFs de standby quentes que apenas ativam quando primários falham
- **HA Ciente da Saúde**: Falha automática quando UPFs perdem associação PFCP ou perdem heartbeats
- **Escalonamento Horizontal**: Distribuir carga entre múltiplos UPFs para aumentar capacidade
- **Alta Disponibilidade**: Distribuição automática evita sobrecarga de um único UPF
- **Implantações Gradativas**: Use pesos para implantações canário (por exemplo, 95% antigo, 5% novo)
- **Otimização de Custos**: Roteie mais tráfego para UPFs de maior capacidade
- **Distribuição Geográfica**: Balancear sessões entre UPFs de borda

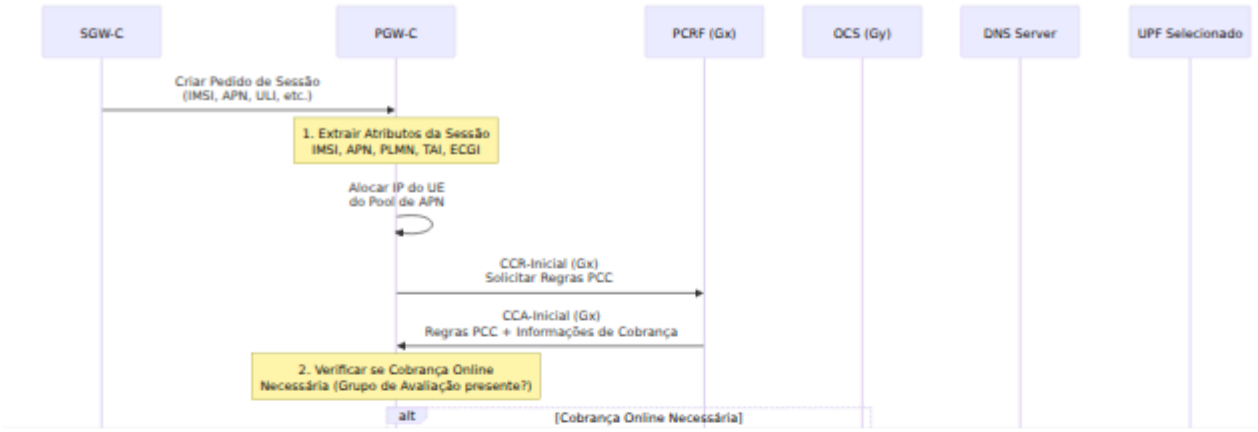
Sobrescritas de PCO (Opções de Configuração de Protocolo):

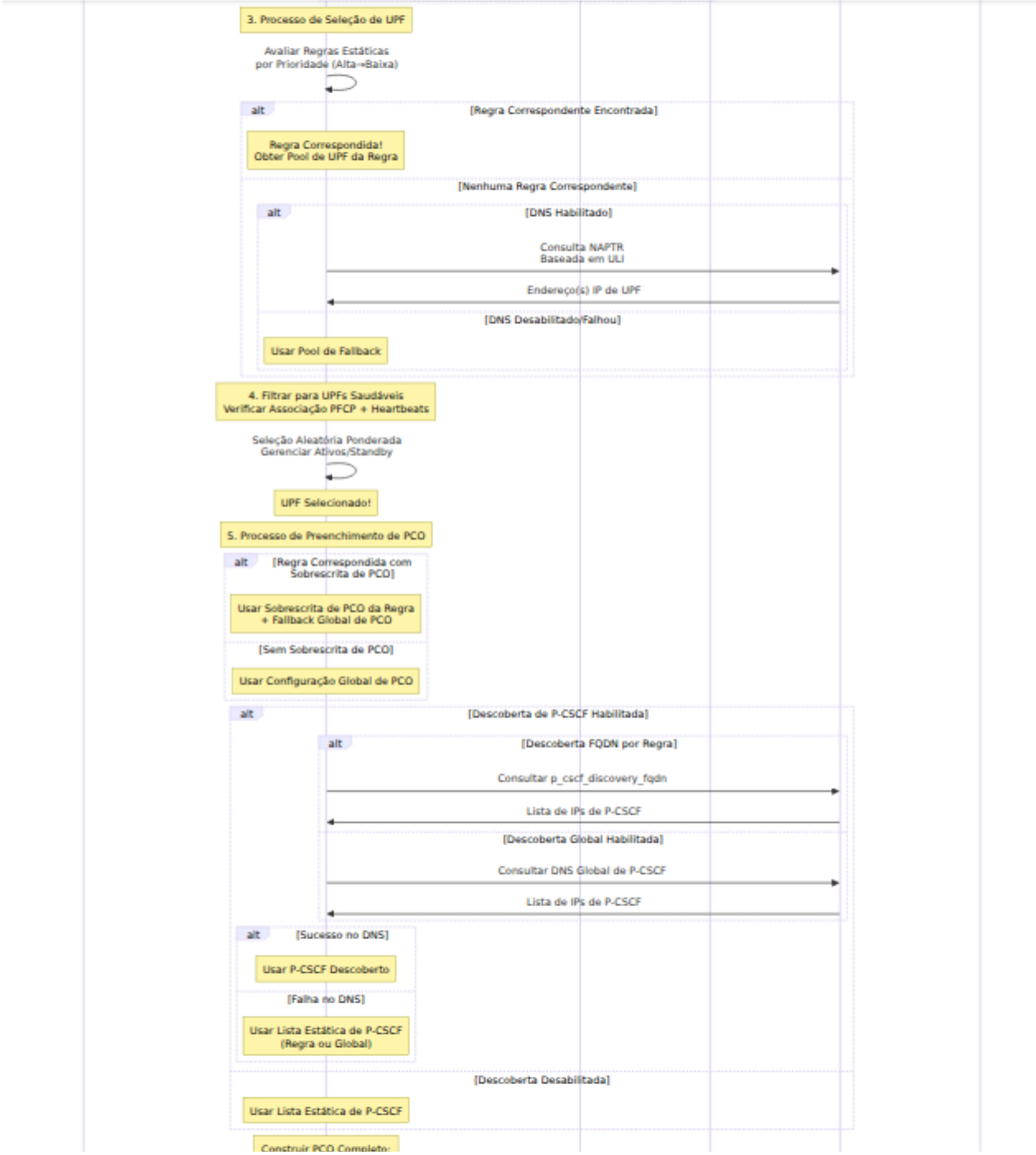
Cada regra de seleção de UPF pode opcionalmente especificar valores de PCO personalizados que sobrescrevem a configuração de PCO padrão para sessões correspondentes. Isso permite que diferentes APNs ou tipos de tráfego recebam diferentes parâmetros de rede.

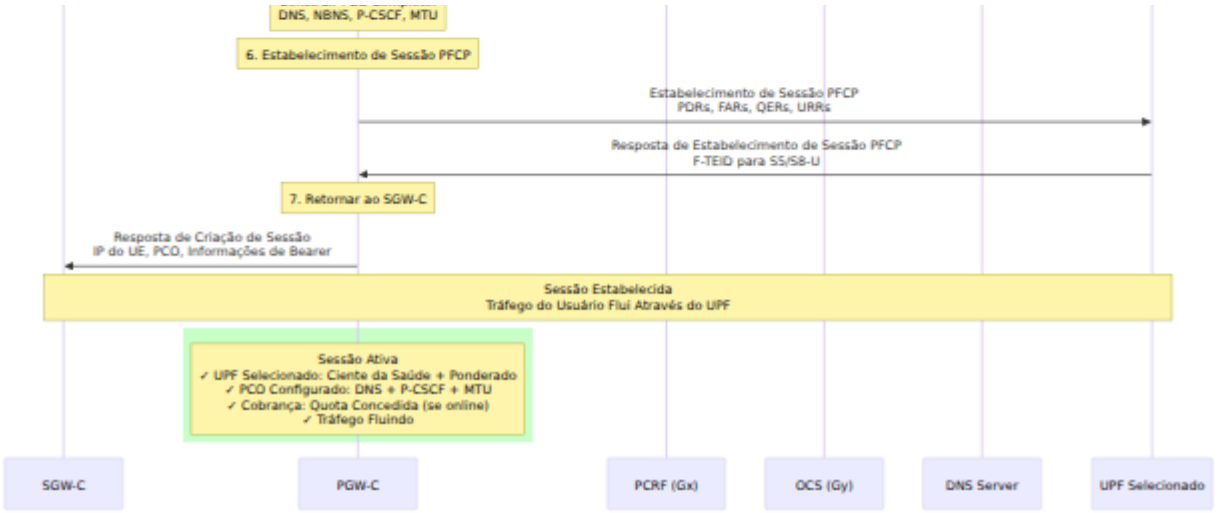
Como Funcionam as Sobrescritas de PCO:

1. **Sobrescritas Parciais**: Especifique apenas os campos de PCO que deseja sobrescrever
2. **Fallback Padrão**: Campos não especificados usam valores da configuração principal `pco`
3. **Específico da Regra**: Cada regra pode ter diferentes sobrescritas de PCO
4. **Mesclagem de Prioridade**: PCO da regra tem prioridade sobre PCO padrão

Hierarquia de Preenchimento de PCO


SGW-C
PGW-C
PCRF (Gx)
OCS (Gy)
DNS Server
UPF Selecionado
Criar Pedido de Sessão (IMSI, APN, ULI, etc.)
1. Extrair Atributos da Sessão IMSI, APN, PLMN, TAI, ECGI
Alocar IP do UE do Pool de APN
CCR-Inicial (Gx) Solicitar Regras PCC
CCA-Inicial (Gx) Regras PCC + Informações de Cobrança
2. Verificar se Cobrança Online Necessária (Grupo de Avaliação presente?)
alt
[Cobrança Online Necessária]


3. Processo de Seleção de UPF
Avaliar Regras Estáticas por Prioridade (Alta→Baixa)
alt
[Regra Correspondente Encontrada]
Regra Correspondida! Obter Pool de UPF da Regra
[Nenhuma Regra Correspondente]
alt
[DNS Habilitado]
Consulta NAPTR Baseada em ULI
Endereço(s) IP de UPF
[DNS Desabilitado/Falhou]
Usar Pool de Fallback
4. Filtrar para UPFs Saudáveis Verificar Associação PFCP + Heartbeats
Seleção Aleatória Ponderada Gerenciar Ativos/Standby
UPF Selecionado!
5. Processo de Preenchimento de PCO
alt
[Regra Correspondida com Sobrescrita de PCO]
Usar Sobrescrita de PCO da Regra + Fallback Global de PCO
[Sem Sobrescrita de PCO]
Usar Configuração Global de PCO
alt
[Descoberta de P-CSCF Habilitada]
alt
[Descoberta FQDN por Regra]
Consultar p_cscf_discovery_fqdn
Lista de IPs de P-CSCF
[Descoberta Global Habilitada]
Consultar DNS Global de P-CSCF
Lista de IPs de P-CSCF
alt
[Sucesso no DNS]
Usar P-CSCF Descoberto
[Falha no DNS]
Usar Lista Estática de P-CSCF (Regra ou Global)
[Descoberta Desabilitada]
Usar Lista Estática de P-CSCF
Construir PCO Completo:



Ordem de Prioridade para Cada Campo de PCO:

1. **Sobrescrita de PCO da Regra** (Maior Prioridade)
2. **Descoberta DNS de P-CSCF** (apenas para endereços P-CSCF)
3. **Configuração Global de PCO** (Menor Prioridade / Fallback)

Exemplo: Sessão IMS Sobrescreve DNS, Regra Empresarial Sobrescreve Tudo

```
Sessão IMS (correspondida pela regra "Tráfego IMS"):
├─ Servidores DNS: DA GLOBAL (não sobrescrito na regra)
├─ P-CSCF: DA DESCOBERTA DNS (p_cscf_discovery_fqdn definido na
regra)
│  └─ Fallback: DA REGRA se DNS falhar
└─ MTU: DA GLOBAL (não sobrescrito na regra)

Sessão Empresarial (correspondida pela regra "Tráfego
Empresarial"):
├─ Servidores DNS: DA REGRA (192.168.1.10, 192.168.1.11)
├─ P-CSCF: DA GLOBAL (não sobrescrito na regra)
└─ MTU: DA REGRA (1500)

Sessão Padrão (nenhuma regra correspondente):
├─ Servidores DNS: DA GLOBAL
├─ P-CSCF: DA GLOBAL ou DNS se descoberta global habilitada
└─ MTU: DA GLOBAL
```

Campos de Sobrescrita de PCO Disponíveis:

- `primary_dns_server_address` - Endereço IP do servidor DNS primário
- `secondary_dns_server_address` - Endereço IP do servidor DNS secundário
- `primary_nbns_server_address` - Endereço IP do servidor WINS primário
- `secondary_nbns_server_address` - Endereço IP do servidor WINS secundário
- `p_cscf_ipv4_address_list` - Lista de endereços IP do servidor P-CSCF (para IMS) - Veja Configuração de PCO e Monitoramento de P-CSCF para descoberta dinâmica de P-CSCF
- `ipv4_link_mtu_size` - Tamanho do MTU em bytes

Descoberta de P-CSCF por Regra:

Além das sobrescritas de PCO, as regras de seleção de UPF podem especificar descoberta dinâmica de P-CSCF:

- `p_cscf_discovery_fqdn` - (String) FQDN para descoberta de P-CSCF baseada em DNS (por exemplo, `"pcscf.mnc380.mcc313.3gppnetwork.org"`)

Quando este parâmetro é definido:

1. PGW-C realiza consulta DNS para o FQDN especificado durante o estabelecimento da sessão
2. O servidor DNS retorna uma lista de endereços IP de P-CSCF
3. Os endereços P-CSCF descobertos são enviados ao UE via PCO
4. Se a consulta DNS falhar, retorna para `p_cscf_ipv4_address_list` da sobrescrita de PCO (se especificado) ou configuração global de PCO
5. Veja Monitoramento de P-CSCF para taxas de sucesso/falha de descoberta

Isso é particularmente útil para:

- **APNs IMS** - Diferentes redes IMS com diferentes servidores P-CSCF
- **Implantações multi-inquilino** - Diferentes empresas com infraestrutura dedicada de P-CSCF
- **Roteamento geográfico** - DNS retorna o P-CSCF mais próximo com base na localização do UE
- **Alta disponibilidade** - DNS retorna automaticamente apenas servidores P-CSCF saudáveis

Exemplo: Tráfego IMS com P-CSCF Personalizado:

```
rules: [
  %{
    name: "Tráfego IMS",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [
      %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
      %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
    ],
    # Descoberta de P-CSCF: Consultar dinamicamente DNS para
endereços de P-CSCF
    # A consulta DNS retorna os IPs de P-CSCF atuais com base
neste FQDN
    p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org",
    # Sessões IMS recebem servidores P-CSCF personalizados (usados
como fallback se DNS falhar)
    pco: %{
      p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
      # DNS, NBNS, MTU usarão defaults da configuração principal
de pco
    }
  }
]
```

Exemplo: Tráfego Empresarial com DNS Personalizado:

```
rules: [
  %{
    name: "Tráfego Empresarial",
    priority: 15,
    match_field: :apn,
    match_regex: "^(enterprise|corporate)\.apn",
    upf_pool: [
      %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
    ],
    # Sessões empresariais recebem DNS corporativo e MTU
personalizado
    pco: %{
      primary_dns_server_address: "192.168.1.10",
      secondary_dns_server_address: "192.168.1.11",
      ipv4_link_mtu_size: 1500
      # P-CSCF, NBNS usarão defaults da configuração principal de
pco
    }
  }
]
```

Exemplo: Sobrescrita Completa (Todos os Campos de PCO):

```
rules: [
  %{
    name: "APN IoT - Totalmente Personalizado",
    priority: 10,
    match_field: :apn,
    match_regex: "^iot\.m2m",
    upf_pool: [
      %{remote_ip_address: "10.100.5.21", remote_port: 8805,
weight: 100}
    ],
    # Sessões IoT recebem PCO totalmente personalizado
    pco: %{
      primary_dns_server_address: "8.8.8.8",
      secondary_dns_server_address: "8.8.4.4",
      primary_nbns_server_address: "10.0.0.100",
      secondary_nbns_server_address: "10.0.0.101",
      p_cscf_ipv4_address_list: [],  # Sem P-CSCF para IoT
      ipv4_link_mtu_size: 1280       # MTU menor para dispositivos
restritos
    }
  }
]
```

Casos de Uso:

- **IMS/VoLTE**: Fornecer servidores P-CSCF específicos do operador para serviços de voz
- **APNs Empresariais**: Roteie tráfego corporativo através de servidores DNS da empresa
- **IoT/M2M**: Usar DNS público e MTU otimizado para dispositivos de baixa largura de banda
- **Roaming**: Fornecer servidores DNS locais para assinantes visitantes
- **Diferenciação de Serviço**: Diferentes parâmetros de rede por tipo de serviço

Seleção de UPF Baseada em DNS Dinâmica:

Habilitar seleção dinâmica de UPF com base nas Informações de Localização do Usuário (ULI) usando consultas NAPTR DNS. As configurações DNS agora são configuradas dentro da seção `upf_selection`.

Nota: Isso fornece seleção de UPF baseada em geografia ou topologia. Veja Interface PFCP para configuração de associação PFCP com UPFs descobertos dinamicamente e Gerenciamento de Sessão para fluxos de estabelecimento de sessão.

```
upf_selection: %{
  # Habilitar seleção baseada em DNS
  dns_enabled: true,

  # Tipos de localização para consultar em ordem de prioridade
  dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],

  # Sufixo DNS para consultas NAPTR 3GPP
  dns_suffix: "epc.3gppnetwork.org",

  # Timeout de consulta DNS em milissegundos
  dns_timeout_ms: 5000,

  # ... regras e fallback_pool ...
}
```

A seleção baseada em DNS funciona da seguinte maneira:

1. **Prioridade**: A seleção DNS é usada apenas quando **NENHUMA regra estática corresponde** (menor prioridade)
2. **Geração de Consulta**: Constrói consultas NAPTR DNS com base na localização do UE:
   - Consulta ECGI: `eci-<hex>.ecgi.epc.mnc&lt;MNC>.mcc&lt;MCC>.epc.3gppnetwork.org`
   - Consulta TAI: `tac-lb<hex>.tac-hb<hex>.tac.epc.mnc&lt;MNC>.mcc&lt;MCC>.epc.3gppnetwork.org`
   - Consultas RAI, SAI, CGI seguem formato semelhante ao 3GPP TS 23.003
3. **Hierarquia de Fallback**: Tenta cada tipo de localização em ordem de prioridade até que uma correspondência seja encontrada
4. **Correspondência de Par**: Resultados DNS são filtrados contra a lista de pares configurados
5. **Seleção**: Escolhe o par correspondente (atualmente a primeira correspondência, seleção baseada em carga em breve)

Exemplo de Registros DNS (configure em seu servidor DNS):

```
; Registro NAPTR para TAC 100 no PLMN 313-380
tac-lb64.tac-hb00.tac.epc.mnc380.mcc313.epc.3gppnetwork.org IN
NAPTR 10 50 "a" "x-3gpp-upf:x-sxb" "" upf-edge-1.example.com.

; Registro A para o UPF
upf-edge-1.example.com IN A 10.100.1.21
```

Casos de Uso:

- **Computação de Borda Multi-Acesso (MEC)**: Roteie sessões para UPFs de borda mais próximos geograficamente
- **Descoberta Dinâmica de UPF**: Adicione/remova UPFs sem reconfigurar o PGW-C
- **Balanceamento de Carga**: Distribua carga entre UPFs com base na localização
- **Fatiamento de Rede**: Roteie diferentes fatias para diferentes UPFs por localização

Monitoramento de Saúde de UPF

Seleção Ciente da Saúde Automática: O PGW-C monitora continuamente a saúde de todos os UPFs e exclui automaticamente UPFs não saudáveis da seleção.

Critérios de Verificação de Saúde

Um UPF é considerado **saudável** quando TODAS as seguintes condições são atendidas:

1. **Associação PFCP Ativa**: O UPF tem uma associação PFCP estabelecida
2. **Responsividade do Heartbeat**: Menos de 3 heartbeats consecutivos perdidos
3. **Processo Vivo**: O processo GenServer do par UPF está em execução

Um UPF é considerado **não saudável** se QUALQUER um dos seguintes for verdadeiro:

- A associação PFCP não está estabelecida (`associated: false`)
- 3 ou mais timeouts consecutivos de heartbeat
- O processo do par UPF falhou ou está não responsivo

Mecanismo de Monitoramento

Para UPFs Configurados (em `upf_selection`):

- O monitoramento de saúde começa imediatamente na inicialização
- A associação PFCP é monitorada continuamente
- Heartbeats são enviados a cada 5 segundos
- O contador `missed_heartbeats_consecutive` rastreia falhas consecutivas
- Todos os UPFs das regras e do pool de fallback são registrados automaticamente

Para UPFs Descobertos por DNS (registro dinâmico):

- Presumido saudável até a primeira tentativa de sessão
- Registrado automaticamente na primeira utilização
- O monitoramento de saúde começa após o registro

Comportamento de Seleção

Modo Ativo/Standby (ao usar `weight: 0`):

1. Filtrar apenas UPFs saudáveis
2. Separar em **ativos** (peso > 0) e **standby** (peso == 0)
3. Usar UPFs ativos se algum estiver saudável
4. Ativar UPFs de standby (tratar como peso 1) se todos os ativos estiverem não saudáveis
5. Retornar ao pool completo se não houver UPFs saudáveis

Modo Balanceado por Carga (todos pesos > 0):

1. Filtrar apenas UPFs saudáveis
2. Realizar seleção aleatória ponderada entre UPFs saudáveis
3. Retornar ao pool completo se não houver UPFs saudáveis

Registro:

```
[debug] Usando pool de UPF ativo (2/3 UPFs saudáveis, 1 standby)
[info] Todos os UPFs ativos inativos, ativando UPFs standby (1
UPFs standby, tratando peso 0 como 1)
[warning] Nenhum UPF saudável no pool (3 totais), usando pool
completo como fallback
```

Verificando a Saúde do UPF

Programaticamente:

```
# Verificar se um UPF específico está saudável
iex> PGW_C.PFCP_Node.is_peer_healthy?({10, 100, 1, 21})
true

# Obter informações detalhadas de saúde
iex> PGW_C.PFCP_Node.get_peer_health({10, 100, 1, 21})
%{
  associated: true,
  missed_heartbeats: 0,
  healthy: true,
  registered: true
}
```

Via Interface Web:

- Navegue até `/upf_selection` no painel de controle
- Veja o status de saúde em tempo real para todos os UPFs em cada pool
- Distintivos de status: Ativo-UP, Standby-Pronto, Ativo-BAIXO, Não Associado
- Distintivos de função: ATIVO (peso > 0), STANDBY (peso == 0), DINÂMICO (descoberto por DNS, não na configuração)
- Contador de misses de heartbeat exibido para UPFs associados

Melhores Práticas de Monitoramento de Saúde

1. **Configure UPFs em upf_selection**: Todos os UPFs nos pools de regras e fallback são monitorados automaticamente

```
upf_selection: %{
  rules: [
    %{
      name: "Tráfego de Internet",
      priority: 10,
      match_field: :apn,
      match_regex: "^internet",
      upf_pool: [
        %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 100}
      ]
    }
  ],
  fallback_pool: [
    %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 100}
  ]
}
# Todos os UPFs automaticamente recebem:
# - heartbeats de 5 segundos
# - Monitoramento de saúde desde a inicialização
# - Nomes gerados automaticamente
```

2. **Use UPFs de standby**: Configure standbys quentes com `weight: 0` para failover automático

```
upf_pool: [
  %{remote_ip_address: "10.1.1.1", remote_port: 8805, weight:
100},  # Ativo
  %{remote_ip_address: "10.1.1.2", remote_port: 8805, weight:
0}     #
```

Formato do Registro de Dados de Cobrança (CDR)

Cobrança Offline para PGW-C

OmniPGW da Omnitouch Network Services

Índice

Visão Geral

O **formato de CDR de Dados (Charging Data Record)** fornece capacidades de cobrança offline para o Plano de Controle do Gateway de Pacotes (PGW-C). Os CDRs são gerados para registrar eventos de sessão de bearer, uso de dados e informações do assinante para fins de faturamento e análise.

Esse formato comum é compatível com os CDRs do SGW-C, garantindo consistência nos registros de cobrança em toda a infraestrutura EPC.

Principais Recursos

- **Formato baseado em CSV** - Valores separados por vírgula simples e legíveis por humanos
- **Gravação baseada em eventos** - Captura eventos de início, atualização e término do bearer
- **Medição de volume** - Registra o uso de dados de uplink e downlink
- **Rotação automática** - Rotação de arquivos configurável com base em intervalos de tempo
- **Conformidade com 3GPP** - Segue 3GPP TS 32.251 (cobrança do domínio PS) e TS 32.298 (codificação de CDR)

Casos de Uso

Caso de Uso	Descrição
Cobrança Offline	Gerar CDRs para faturamento pós-pago
Análise	Analisar padrões de uso dos assinantes
Rastro de Auditoria	Rastrear todos os eventos de sessão de bearer
Planejamento de Capacidade	Monitorar a utilização de recursos da rede
Solução de Problemas	Depurar problemas de sessão e bearer

Formato do Arquivo CDR

Convenção de Nomenclatura de Arquivo

```
<epoch_timestamp>
```

Exemplo:

```
1726598022
```

O nome do arquivo é o timestamp Unix epoch (em segundos) de quando o arquivo foi criado.

Localização do Arquivo

Diretório padrão:

- PGW-C: `/var/log/pgw_c/cdrs/`

Configurável via parâmetro `cdr_directory` em config/runtime.exs.

Cabeçalho do Arquivo

Cada arquivo CDR começa com um cabeçalho de várias linhas contendo metadados:

```
# Arquivo CDR de Dados:
# Hora de Início do Arquivo: HH:MM:SS (unix_timestamp)
# Hora de Fim do Arquivo: HH:MM:SS (unix_timestamp)
# Nome do Gateway: <gateway_name>
#
epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,eci
```

Campos do Cabeçalho:

- **Hora de Início do Arquivo** - Quando o arquivo CDR foi criado (legível por humanos e timestamp Unix)
- **Hora de Fim do Arquivo** - Quando a rotação do arquivo ocorrerá (legível por humanos e timestamp Unix)
- **Nome do Gateway** - Identificador para a instância PGW-C (configurado via parâmetro `pgw_name`)
- **Cabeçalhos das Colunas** - Nomes dos campos CSV para os registros de dados

---

Campos do CDR

Resumo dos Campos

Posição	Nome do Campo	Tipo	Descrição
0	epoch	inteiro	Timestamp do evento (segundos Unix epoch)
1	imsi	string	Identidade Internacional do Assinante Móvel
2	event	string	Tipo de evento CDR (por exemplo, "default_bearer_start")
3	charging_id	inteiro	Identificador único de cobrança para o bearer
4	msisdn	string	Número ISDN da Estação Móvel (número de telefone)
5	ue_imei	string	Identidade Internacional do Equipamento Móvel
6	timezone_raw	string	Fuso horário do UE (reservado, atualmente vazio)
7	plmn	inteiro	Identificador da Rede Móvel Pública
8	tac	inteiro	Código da Área de Rastreamento
9	eci	inteiro	Identificador da Célula E-UTRAN
10	sgw_ip	string	Endereço IP do plano de controle S5/S8 do SGW-C

Posição	Nome do Campo	Tipo	Descrição
11	ue_ip	string	Endereço IP do UE (formato IPv4|IPv6)
12	pgw_ip	string	Endereço IP do plano de controle S5/S8 do PGW-C
13	apn	string	Nome do Ponto de Acesso
14	qci	inteiro	Identificador da Classe de QoS
15	octets_in	inteiro	Volume de dados de downlink (bytes)
16	octets_out	inteiro	Volume de dados de uplink (bytes)

Eventos do CDR

Tipos de Eventos

Os CDRs são gerados para três tipos de eventos:

Tipo de Evento	Formato	Descrição	Quando Gera
Início do Bearer	`<type>_bearer_start`	Estabelecimento do bearer	Resposta de Cria de Sessão envia
Atualização do Bearer	`<type>_bearer_update`	Relatório de uso durante a sessão	Relatórios de us periódicos do pl de usuário
Término do Bearer	`<type>_bearer_end`	Término do bearer	Solicitação/Resp de Exclusão de Sessão

Tipos de Bearer:

- `default` - Bearer padrão (um por conexão PDN)
- `dedicated` - Bearer dedicado (zero ou mais por conexão PDN)

Exemplos de Eventos

```
default_bearer_start      - Bearer padrão estabelecido
default_bearer_update     - Atualização de uso do bearer padrão
default_bearer_end        - Bearer padrão terminado
dedicated_bearer_start    - Bearer dedicado estabelecido
dedicated_bearer_update   - Atualização de uso do bearer dedicado
dedicated_bearer_end      - Bearer dedicado terminado
```

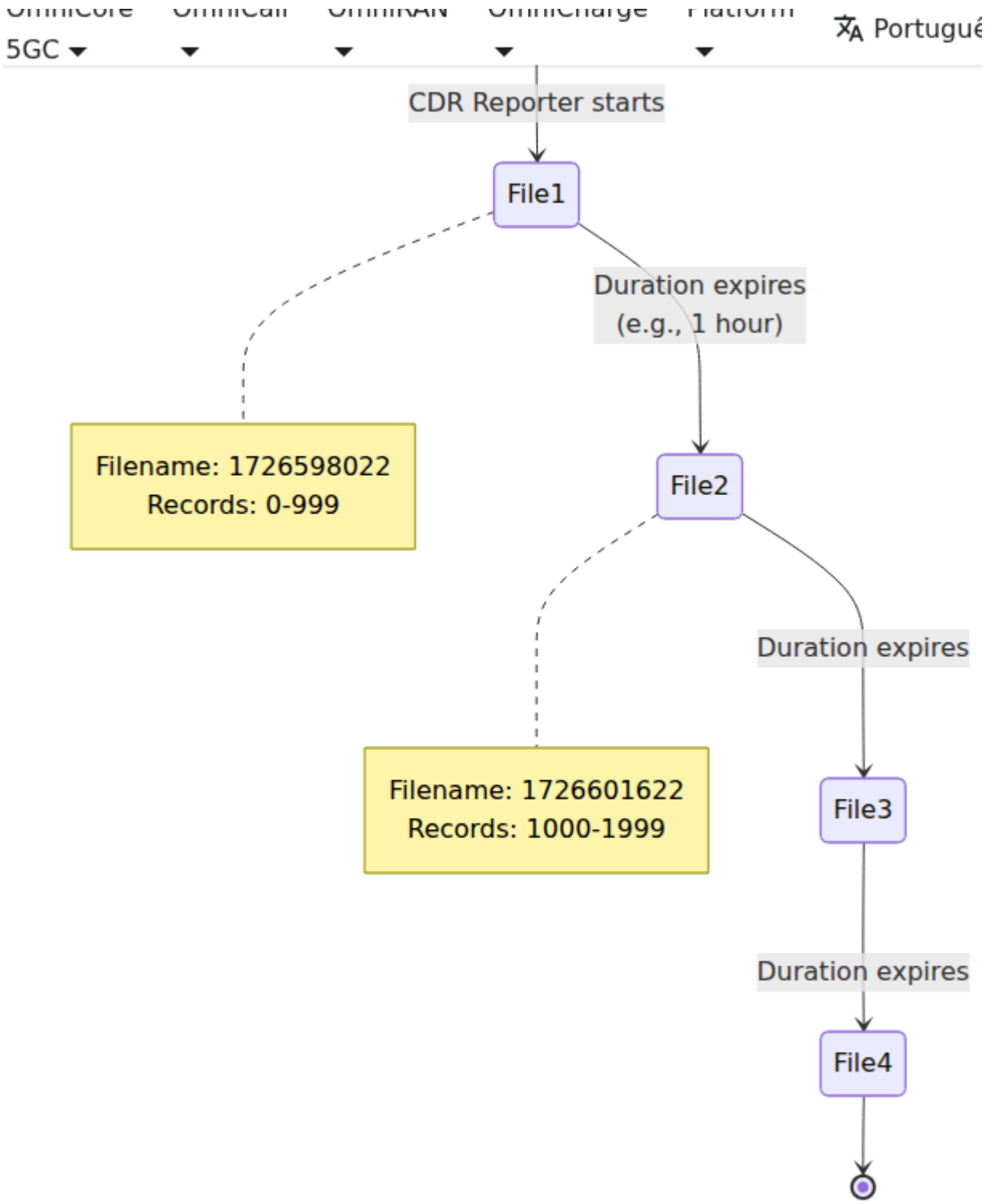
Estrutura do Arquivo

Exemplo de Arquivo CDR

```
# Arquivo CDR de Dados:
# Hora de Início do Arquivo: 18:53:42 (1726598022)
# Hora de Fim do Arquivo: 19:53:42 (1726601622)
# Nome do Gateway: sgw-c-prod-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,e
1726598022,310260123456789,default_bearer_start,12345,15551234567,123
1726598322,310260123456789,default_bearer_update,12345,15551234567,12
1726598622,310260123456789,default_bearer_update,12345,15551234567,12
1726598922,310260123456789,default_bearer_end,12345,15551234567,12345
```

Rotação de Arquivo

Os arquivos CDR são automaticamente rotacionados com base na duração configurada:



Processo de Rotação:

1. Fechar o arquivo CDR atual
2. Criar um novo arquivo com o timestamp atual
3. Escrever o cabeçalho no novo arquivo
4. Continuar gravando CDRs no novo arquivo

Configuração

Parâmetros de Configuração

A geração de CDR do PGW-C é configurada em `config/runtime.exs`:

Parâmetro	Tipo	Descrição	Padrão	Reco
`pgw_name`	string	Identificador da instância PGW (aparece nos cabeçalhos do CDR)	"omni-pgw01"	Usar nom ID da inst
`cdr_file_duration`	inteiro	Intervalo de rotação do arquivo (ms)	3600000	3600000
`cdr_directory`	string	Caminho do diretório de saída do CDR	"/tmp/pgw_c"	`/var/log`
`usage_report_interval`	inteiro	Intervalo de relatório URR (ms) - com que frequência o PGW-U envia relatórios de uso	60000	60000 (1

Exemplos de Configuração

Configuração Mínima (config/runtime.exs):

```
config :pgw_c,
  # Configuração do arquivo CDR
  pgw_name: "omni-pgw01",
  cdr_file_duration: 3_600_000,           # 1 hora
  cdr_directory: "/var/log/pgw_c/cdrs",

  # Configuração URR (dispara relatórios de uso do PGW-U)
  usage_report_interval: 60_000           # 60 segundos
```

Produção:

```
config :pgw_c,
  pgw_name: "pgw-c-prod-01",
  cdr_file_duration: 3_600_000,           # Rotação de 1 hora
  cdr_directory: "/var/log/pgw_c/cdrs",
  usage_report_interval: 60_000           # Atualizações de 1
minuto
```

Desenvolvimento:

```
config :pgw_c,
  pgw_name: "pgw-c-dev",
  cdr_file_duration: 300_000,             # Rotação de 5 minutos
para testes
  cdr_directory: "/tmp/pgw_c_cdrs",
  usage_report_interval: 30_000           # Atualizações de 30
segundos para testes mais rápidos
```

Alto Volume:

```
config :pgw_c,
  pgw_name: "pgw-c-prod-heavy",
  cdr_file_duration: 1_800_000,           # Rotação de 30 minutos
  cdr_directory: "/mnt/fast-storage/cdrs",
  usage_report_interval: 300_000          # Atualizações de 5
minutos (reduzir sobrecarga)
```

URR (Regras de Relatório de Uso)

O PGW-C usa **URRs de PFCP (Regras de Relatório de Uso)** para acionar relatórios de uso do PGW-U. Quando um limite de URR é alcançado ou o tempo expira, o PGW-U envia uma Solicitação de Relatório de Sessão contendo dados de uso, o que aciona a geração de CDR.

Como Funciona a Configuração do URR:

1. `usage_report_interval` (em ms) é convertido em segundos para o limite de tempo do PFCP
2. O PGW-C cria URR com limite de tempo durante o estabelecimento da sessão
3. O PGW-U envia relatórios de uso periódicos no intervalo configurado
4. Cada relatório de uso aciona um evento CDR `bearer_update`
5. O relatório de uso final (na exclusão da sessão) aciona um evento CDR `bearer_end`

Exemplo: `usage_report_interval: 60_000` significa:

- O PGW-U relata uso a cada 60 segundos
- Eventos de atualização do CDR gerados a cada 60 segundos
- Rastreamento granular de uso para faturamento

Definição do Tipo de URR:

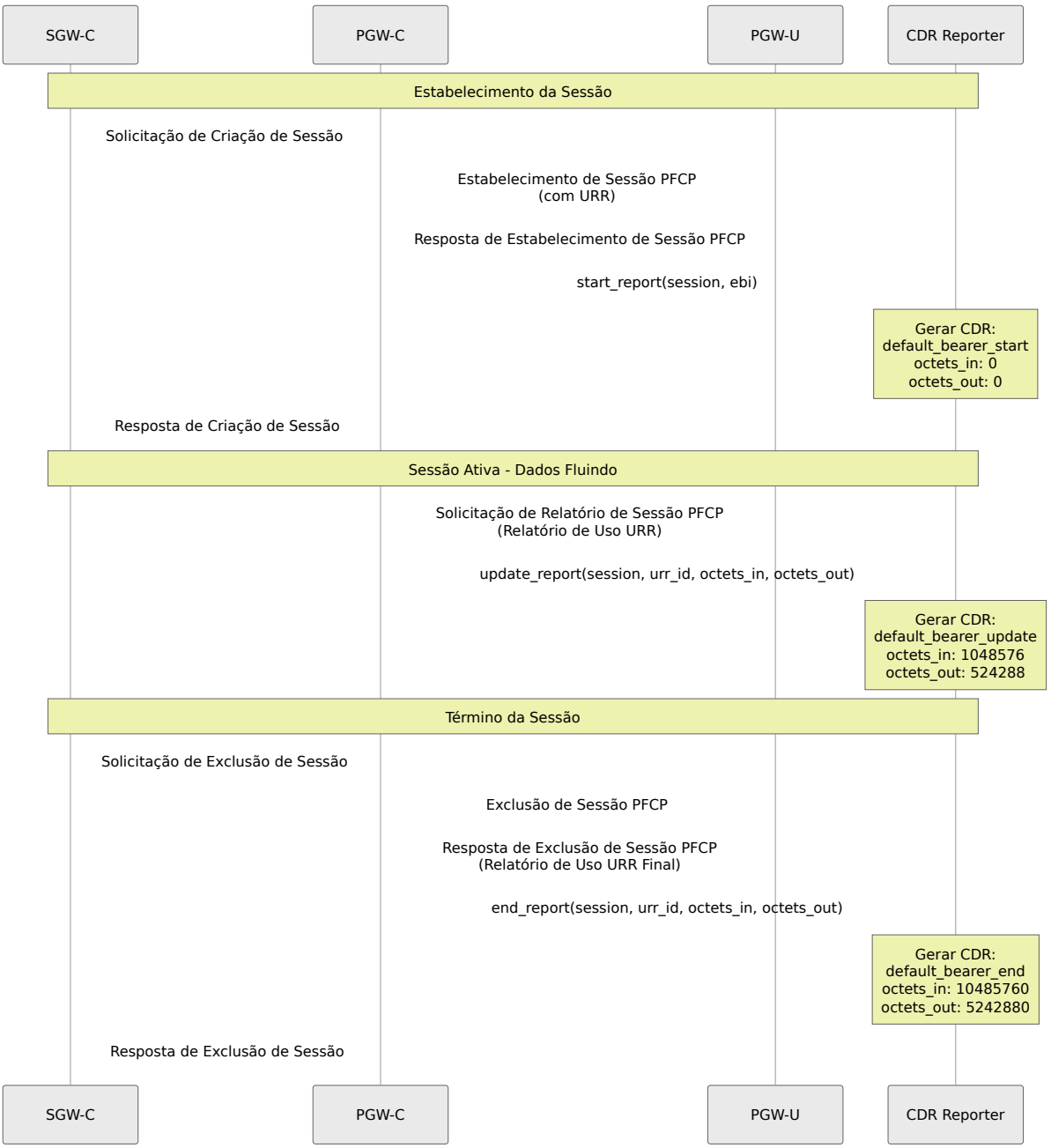
```
# lib/core/session/types.ex
defmodule PGW_C.Session.Types.URR do
  typedstruct do
    field :urr_id, non_neg_integer()
    field :measurement_method, :duration | nil
    field :reporting_triggers, :time_threshold | nil
    field :time_threshold, non_neg_integer() | nil  # segundos
  end
end
```

Veja a Documentação da Interface PFCP para detalhes do URR PFCP e lib/core/session/impl/procedures.ex:468 para criação do URR durante o estabelecimento da sessão.

Fluxo de Geração do CDR

Eventos de CDR do Ciclo de Vida do Bearer

Geração de CDR do PGW-C:



Eventos de Geração do CDR

1. Início do Bearer:

- **Quando:** Resposta de Criação de Sessão é enviada
- **Propósito:** Registra o estabelecimento do bearer com uso zero
- **octets_in:** 0
- **octets_out:** 0

2. Atualização do Bearer:

- **Quando:** Solicitação de Relatório de Sessão PFCP recebida do PGW-U (relatório de uso URR)
- **Propósito:** Registra o uso incremental de dados
- **octets_in:** Bytes de downlink acumulados desde o início do bearer
- **octets_out:** Bytes de uplink acumulados desde o início do bearer
- **Gatilho:** Limite de tempo do URR expira (configurado via `usage_report_interval`)

3. Término do Bearer:

- **Quando:** Resposta de Exclusão de Sessão PFCP recebida do PGW-U (com relatório de uso final)
- **Propósito:** Registra o uso final de dados antes do término da sessão
- **octets_in:** Total final de bytes de downlink
- **octets_out:** Total final de bytes de uplink

Detalhes dos Campos

1. epoch (Timestamp)

Tipo: Timestamp Unix epoch (segundos)

Descrição: O momento em que o evento CDR ocorreu

Exemplo:

```
1726598022  → 2025-09-17 18:53:42 UTC
```

---

2. imsi (Identidade do Assinante)

Tipo: String (até 15 dígitos)

Formato: MCCMNC + MSIN

Descrição: Identidade Internacional do Assinante Móvel que identifica exclusivamente o assinante

Exemplo:

```
310260123456789
  └─┘ └─┘ └─────────┘
   MCC  MNC     MSIN
   (310)(260) (123456789)
```

Fonte: Contexto do UE, recebido na Solicitação de Criação de Sessão

---

3. event (Tipo de Evento do CDR)

Tipo: String

Formato: `<bearer_type>_bearer_<event>`

Valores:

- `default_bearer_start`
- `default_bearer_update`
- `default_bearer_end`
- `dedicated_bearer_start`
- `dedicated_bearer_update`
- `dedicated_bearer_end`

Determinação:

- Se EBI (EPS Bearer ID) é igual a LBI (Linked Bearer ID): `default`
- Se EBI não é igual a LBI: `dedicated`

Fonte: Contexto do bearer (comparação EBI vs LBI)

---

4. charging_id (Identificador de Cobrança)

Tipo: Inteiro não assinado de 32 bits

Descrição: Identificador único para correlação de cobrança entre elementos da rede

Exemplo:

```
12345
```

Fonte: Atribuído pelo PGW-C, recebido na Resposta de Criação de Sessão

Uso:

- Correlaciona eventos de cobrança entre SGW e PGW
- Usado nas interfaces de cobrança Diameter Gy/Gz
- Único por bearer

---

5. msisdn (Número de Telefone)

Tipo: String (formato E.164)

Descrição: Número ISDN da Estação Móvel (número de telefone do assinante)

Formato: Código do país + número nacional

Exemplo:

```
15551234567
 └┘└─────┘
  CC  Nacional
  (1) (5551234567)
```

Fonte: Contexto do UE, tipicamente do HSS via MME

---

6. ue_imei (Identidade do Equipamento)

Tipo: String (15 dígitos)

Formato: TAC (8) + SNR (6) + Spare (1)

Descrição: Identidade Internacional do Equipamento Móvel (identificador do dispositivo)

Exemplo:

```
123456789012345
└──────┘└────┘└
   TAC   SNR S
```

Fonte: Contexto do UE, recebido do MME

---

7. timezone_raw (Fuso Horário do UE)

Tipo: String (atualmente reservado/vazio)

Descrição: Campo reservado para informações de fuso hor��rio do UE

Status Atual: Não populado (campo vazio no CSV)

Uso Futuro: Pode incluir deslocamento de fuso horário e sinalizador de horário de verão

Exemplo:

```
,  (campo vazio)
```

---

8. plmn (Identificador da Rede)

Tipo: Inteiro (formato legado)

Descrição: Identificador da Rede Móvel Pública codificado como hex little-endian

Processo de Codificação:

```
MCC: 505, MNC: 57
  ↓
"50557"
  ↓
Trocar pares: "055570"
  ↓
Hex para decimal: 0x055570 = 349552
```

Exemplo:

```
349552  → MCC: 505, MNC: 57
```

Fonte: Informações de localização do UE do MME

Nota: Este é um formato de codificação legado para compatibilidade retroativa

---

9. tac (Código da Área de Rastreamento)

Tipo: Inteiro não assinado de 16 bits

Descrição: O Código da Área de Rastreamento identifica a área de rastreamento onde o UE está localizado

Intervalo: 0 - 65535

Exemplo:

```
1234
```

Fonte: Informações de localização do UE, recebidas do MME na Solicitação de Criação de Sessão

Uso:

- Identifica a área de gerenciamento de mobilidade
- Usado para paginação e atualizações de localização
- Parte do TAI (Identidade da Área de Rastreamento)

---

10. eci (Identificador da Célula E-UTRAN)

Tipo: Inteiro não assinado de 28 bits

Descrição: O Identificador da Célula E-UTRAN identifica exclusivamente a célula que atende o UE

Formato: ID do eNodeB (20 bits) + ID da Célula (8 bits)

Intervalo: 0 - 268.435.455

Exemplo:

```
5678
```

Fonte: Informações de localização do UE do MME

Uso:

- Identifica a torre de celular e setor específicos
- Usado para transferência e gerenciamento de mobilidade
- Informações de localização granular

---

11. sgw_ip (IP do Plano de Controle do SGW)

Tipo: String (endereço IPv4 ou IPv6)

Descrição: Endereço IP do plano de controle S5/S8 do SGW-C (F-TEID)

Formato: Decimal pontuado (IPv4) ou hex com dois pontos (IPv6)

Exemplo:

```
10.0.0.15       (IPv4)
2001:db8::15    (IPv6)
```

Fonte: Configuração local, atribuída à interface S5/S8

---

12. ue_ip (Endereço IP do UE)

Tipo: String (formato IPv4|IPv6)

Descrição: Endereço IP atribuído ao UE para a conexão PDN

Formato: `<ipv4>|<ipv6>`

Exemplos:

```
172.16.1.100|                       (somente IPv4)
|2001:db8::1                        (somente IPv6)
172.16.1.100|2001:db8::1          (Dual-stack)
```

Fonte: Alocação de Endereço PDN (PAA) do PGW-C

Notas:

- IPv4 vazio: Nenhum endereço IPv4 alocado
- IPv6 vazio: Nenhum endereço IPv6 alocado
- Ambos presentes: Conexão PDN dual-stack

---

13. pgw_ip (IP do Plano de Controle do PGW)

Tipo: String (endereço IPv4 ou IPv6)

Descrição: Endereço IP do plano de controle S5/S8 do PGW-C (F-TEID remoto)

Formato: Decimal pontuado (IPv4) ou hex com dois pontos (IPv6)

Exemplo:

```
10.0.0.20       (IPv4)
2001:db8::20    (IPv6)
```

Fonte: Recebido na Resposta de Criação de Sessão do PGW-C

---

14. apn (Nome do Ponto de Acesso)

Tipo: String (até 100 caracteres)

Descrição: Nome do Ponto de Acesso que identifica a rede externa (PDN)

Formato: Formato de rótulo semelhante ao DNS

Exemplos:

```
internet
ims
mms
enterprise.corporate
```

Fonte: Recebido na Solicitação de Criação de Sessão do MME

Uso:

- Determina a qual rede externa se conectar
- Impulsiona políticas e regras de cobrança
- Pode determinar o pool de endereços IP

---

15. qci (Identificador da Classe de QoS)

Tipo: Inteiro não assinado de 8 bits

Descrição: O Identificador da Classe de QoS define a qualidade de serviço do bearer

Intervalo: 1 - 9 (padronizado), 128-254 (específico do operador)

Valores de QCI Padronizados:

QCI	Tipo de Recurso	Prioridade	Atraso de Pacote	Perda de Pacote	Serviço Exemplo
1	GBR	2	100 ms	10^-2	Voz Conversacional
2	GBR	4	150 ms	10^-3	Vídeo Conversacional
3	GBR	3	50 ms	10^-3	Jogos em Tempo Real
4	GBR	5	300 ms	10^-6	Vídeo Não Conversacional
5	Non-GBR	1	100 ms	10^-6	Sinalização IMS
6	Non-GBR	6	300 ms	10^-6	Vídeo (bufferizado)
7	Non-GBR	7	100 ms	10^-3	Voz, Vídeo, Jogos
8	Non-GBR	8	300 ms	10^-6	Vídeo (bufferizado)
9	Non-GBR	9	300 ms	10^-6	Bearer Padrão

Exemplo:

```
9  → Bearer padrão (melhor esforço)
```

Fonte: Parâmetros de QoS do bearer do PGW-C

---

16. octets_in (Volume de Downlink)

Tipo: Inteiro não assinado de 64 bits

Descrição: Número de bytes transmitidos na direção de downlink (rede → UE)

Unidades: Bytes

Exemplo:

```
1048576  → 1 MB de downlink
```

Fonte: Medição de Volume PFCP do PGW-U (via relatórios de uso URR)

Notas:

- Acumulativo para eventos `update`
- Total final para eventos `end`
- Sempre 0 para eventos `start`
- Relatórios acionados pelo limite de tempo do URR (configurado via `usage_report_interval`)

---

17. octets_out (Volume de Uplink)

Tipo: Inteiro não assinado de 64 bits

Descrição: Número de bytes transmitidos na direção de uplink (UE → rede)

Unidades: Bytes

Exemplo:

```
524288  → 512 KB de uplink
```

Fonte: Medição de Volume PFCP do PGW-U (via relatórios de uso URR)

Notas:

- Acumulativo para eventos `update`
- Total final para eventos `end`
- Sempre 0 para eventos `start`
- Relatórios acionados pelo limite de tempo do URR (configurado via `usage_report_interval`)

Exemplos

Exemplo 1: Sessão Básica com Atualização Única

Linha do Tempo:

1. Bearer estabelecido
2. 5 minutos depois: Atualização de uso (10 MB down, 5 MB up)
3. Sessão terminada

Saída do CDR:

```
# Arquivo CDR de Dados:
# Hora de Início do Arquivo: 10:00:00 (1726570800)
# Hora de Fim do Arquivo: 11:00:00 (1726574400)
# Nome do Gateway: pgw-c-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,e
1726570800,310260111111111,default_bearer_start,10001,15551111111,111
1726571100,310260111111111,default_bearer_update,10001,15551111111,11
1726571400,310260111111111,default_bearer_end,10001,15551111111,11111
```

Exemplo 2: Sessão Dual-Stack com Múltiplas Atualizações

Linha do Tempo:

1. Bearer dual-stack estabelecido (IPv4 + IPv6)
2. Múltiplas atualizações de uso
3. Sessão terminada

Saída do CDR:

```
1726570800,310260222222222,default_bearer_start,10002,15552222222,222
1726571100,310260222222222,default_bearer_update,10002,15552222222,22
1726571400,310260222222222,default_bearer_update,10002,15552222222,22
1726571700,310260222222222,default_bearer_update,10002,15552222222,22
1726572000,310260222222222,default_bearer_end,10002,15552222222,22222
```

Exemplo 3: Sessão com Bearer Dedicado

Linha do Tempo:

1. Bearer padrão estabelecido (QCI 9)
2. Bearer dedicado criado para vídeo (QCI 6)
3. Atualizações de uso para ambos os bearers
4. Bearer dedicado excluído
5. Bearer padrão terminado

Saída do CDR:

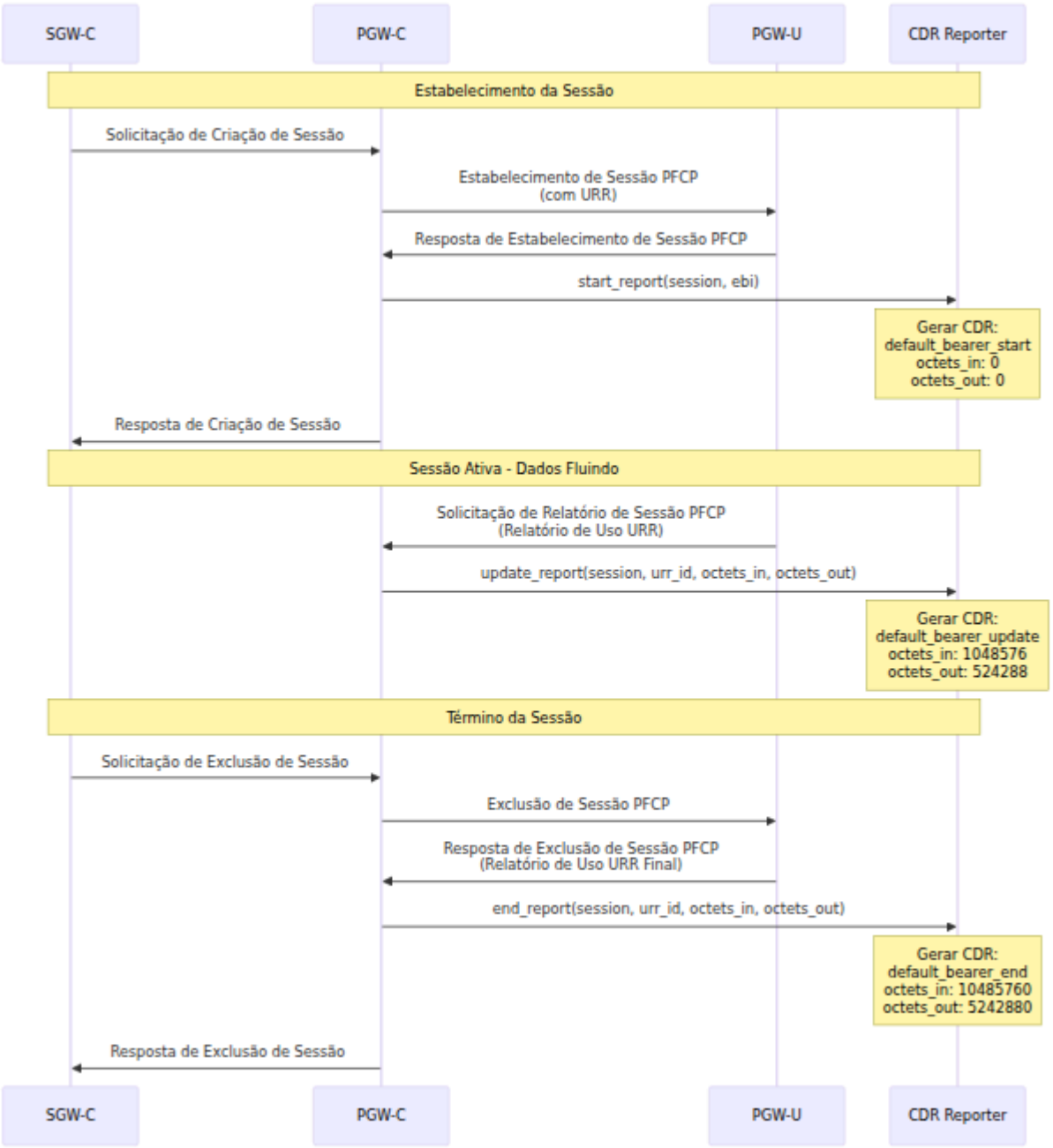
```
1726570800,310260333333333,default_bearer_start,10003,15553333333,333
1726571100,310260333333333,dedicated_bearer_start,10004,15553333333,3
1726571400,310260333333333,default_bearer_update,10003,15553333333,33
1726571400,310260333333333,dedicated_bearer_update,10004,15553333333,
1726571700,310260333333333,dedicated_bearer_end,10004,15553333333,333
1726572000,310260333333333,default_bearer_end,10003,15553333333,33333
```

Análise:

- Bearer padrão (10003) transporta tráfego de fundo (10 MB down, 4 MB up)
- Bearer dedicado (10004) transporta tráfego de vídeo (200 MB down, 2 MB up)
- Diferentes valores de QCI (9 vs 6) refletem diferentes tratamentos de QoS

Integração

Pipeline de Processamento de CDR



Métodos de Coleta de CDR

1. Coleta Baseada em Arquivo:

```
# Monitorar diretório CDR (PGW-C)
inotifywait -m /var/log/pgw_c/cdrs/ -e close_write | while read
path action file; do
    # Rotação de arquivo concluída, processar CDR
    process_cdr "$path$file"
done
```

2. Streaming em Tempo Real:

```
# Tail e stream para pipeline de processamento
tail -F /var/log/pgw_c/cdrs/* | process_cdr_stream
```

Documentação Relacionada

- Gerenciamento de Sessão - Ciclo de vida da sessão e gatilhos de CDR
- Interface PFCP - Relatório de uso do PGW-U via URRs
- Guia de Monitoramento - Métricas de geração de CDR e alertas
- Guia de Configuração - Parâmetros de configuração de CDR e URR
- Interface Diameter Gx - Controle de políticas para valores de QCI em CDRs
- Interface Diameter Gy - Integração de cobrança online

Referências 3GPP

- TS 32.251 - Cobrança do domínio Pacote (PS)
- TS 29.274 - Sistema de Pacotes Evoluído 3GPP (EPS); protocolo GTP-C
- TS 29.244 - Interface entre nós de CP e UP (PFCP) - **suporte a URR**
- TS 32.298 - Codificação de CDR

Formato do CDR - *Registros de Cobrança Offline para PGW-C*

Desenvolvido pela Omnitouch Network Services

Versão da Documentação: 1.0 **Última Atualização:** 2025-12-28

Documentação da Interface Gx do Diameter

Interface da Função de Regras de Política e Cobrança (PCRF)

Índice

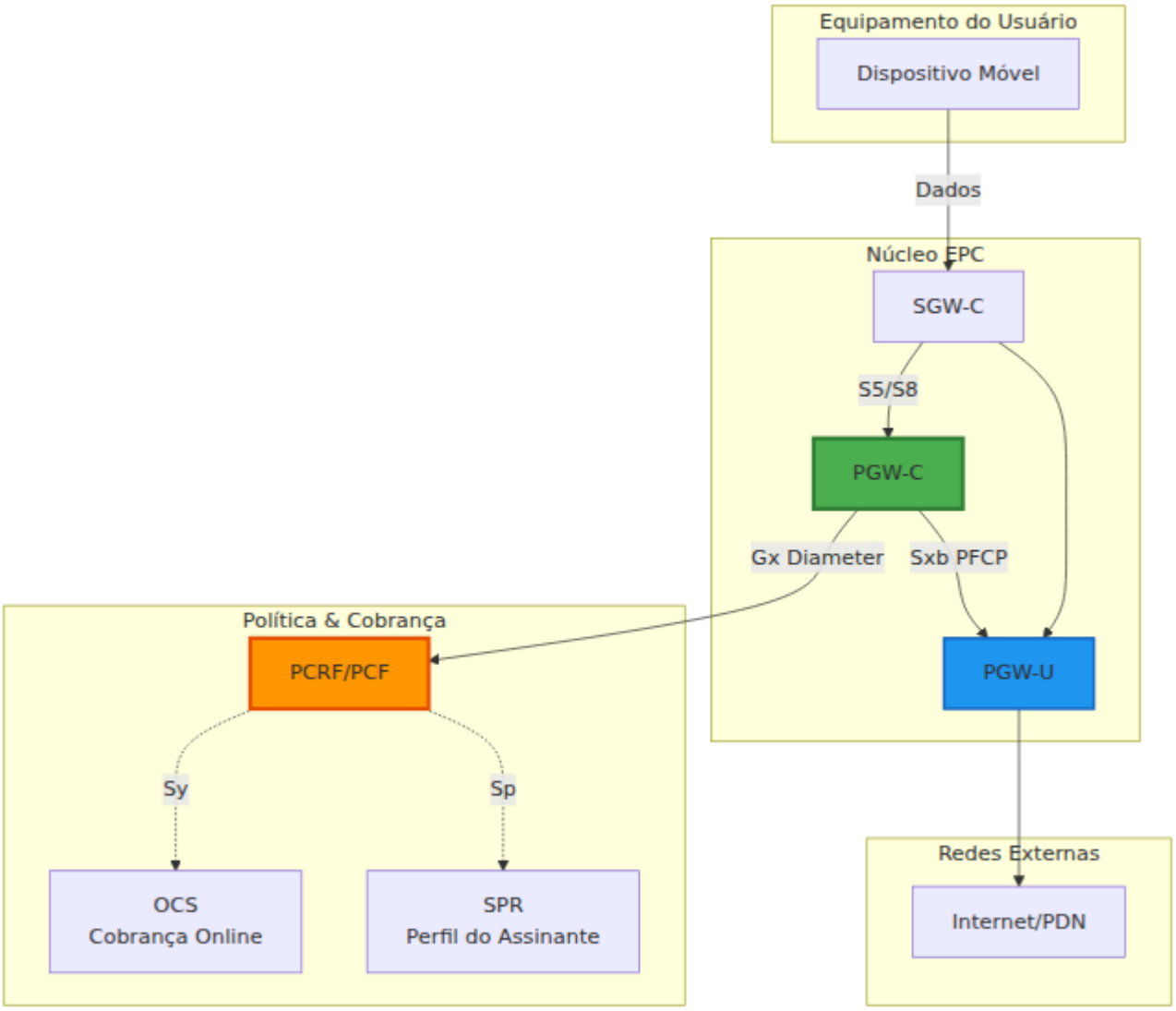
Visão Geral

A **interface Gx** conecta o PGW-C à **PCRF (Função de Regras de Política e Cobrança)** ou **PCF (Função de Controle de Política)** em redes 5G. Esta interface permite:

- **Controle de Política Dinâmico** - Aplicação de QoS e políticas em tempo real
- **Controle de Cobrança** - Autorização de crédito e rastreamento de uso
- **Consciência de Serviço** - Diferenciação de tráfego em nível de aplicação

- **Gerenciamento de Perfil do Assinante** - Aplicação de políticas por usuário

Gx na Arquitetura da Rede



Funções Principais

Função	Descrição
Provisionamento de Política	PCRF fornece regras de PCC definindo como lidar com o tráfego
Controle de QoS	Ajuste dinâmico de taxas de bits e parâmetros de QoS
Controle de Cobrança	Autorização de crédito para cenários pré-pagos/pós-pagos
Controle de Gating	Habilitar/desabilitar fluxos de tráfego com base na política
Monitoramento de Uso	Rastrear consumo de dados por serviço

Noções Básicas da Interface Gx

Referência 3GPP

- **Especificação:** 3GPP TS 29.212
- **ID da Aplicação Diameter:** 16777238 (Gx)
- **Protocolo:** Protocolo Base Diameter (RFC 6733)

Conceito de Sessão

Cada conexão PDN do UE tem uma **sessão Gx** correspondente identificada por um **Session-ID**. Esta sessão:

- Criada quando o UE se conecta (CCR-Initial)
- Atualizada durante a vida útil da conexão (CCR-Update) - opcional
- Terminada quando o UE se desconecta (CCR-Termination)

Formato do ID da Sessão

```
Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]
Exemplo: omni-
pgw_c.epc.mnc999.mcc999.3gppnetwork.org;1234567890;98765
```

Componentes:

- **Origin-Host:** Identidade Diameter do PGW-C
- **high32:** 32 bits altos do identificador único
- **low32:** 32 bits baixos do identificador único

Protocolo Diameter

Estrutura da Mensagem

As mensagens Diameter são codificadas em binário com a seguinte estrutura:

```
Cabeçalho Diameter (20 bytes)
├── Versão (1 byte) = 1
├── Comprimento da Mensagem (3 bytes)
├── Flags (1 byte)
│   ├── R: Requisição (1) / Resposta (0)
│   ├── P: Proxiável
│   ├── E: Erro
│   └── T: Potencialmente retransmitido
├── Código do Comando (3 bytes)
├── ID da Aplicação (4 bytes) = 16777238 (Gx)
├── ID Hop-by-Hop (4 bytes)
└── ID End-to-End (4 bytes)

AVPs (Pares Atributo-Valor)
├── Cabeçalho AVP
│   ├── Código AVP
│   ├── Flags (V, M, P)
│   ├── Comprimento AVP
│   └── ID do Fornecedor (opcional)
└── Dados AVP
```

Conceitos Chave do Diameter

AVP (Par Atributo-Valor):

- Unidade de dados básica no Diameter
- Contém um código, flags e valor
- Pode ser aninhado (AVP Agrupado)

Comando:

- Par Requisição/Resposta
- CCR (Requisição de Controle de Crédito) / CCA (Resposta de Controle de Crédito)

Códigos de Resultado:

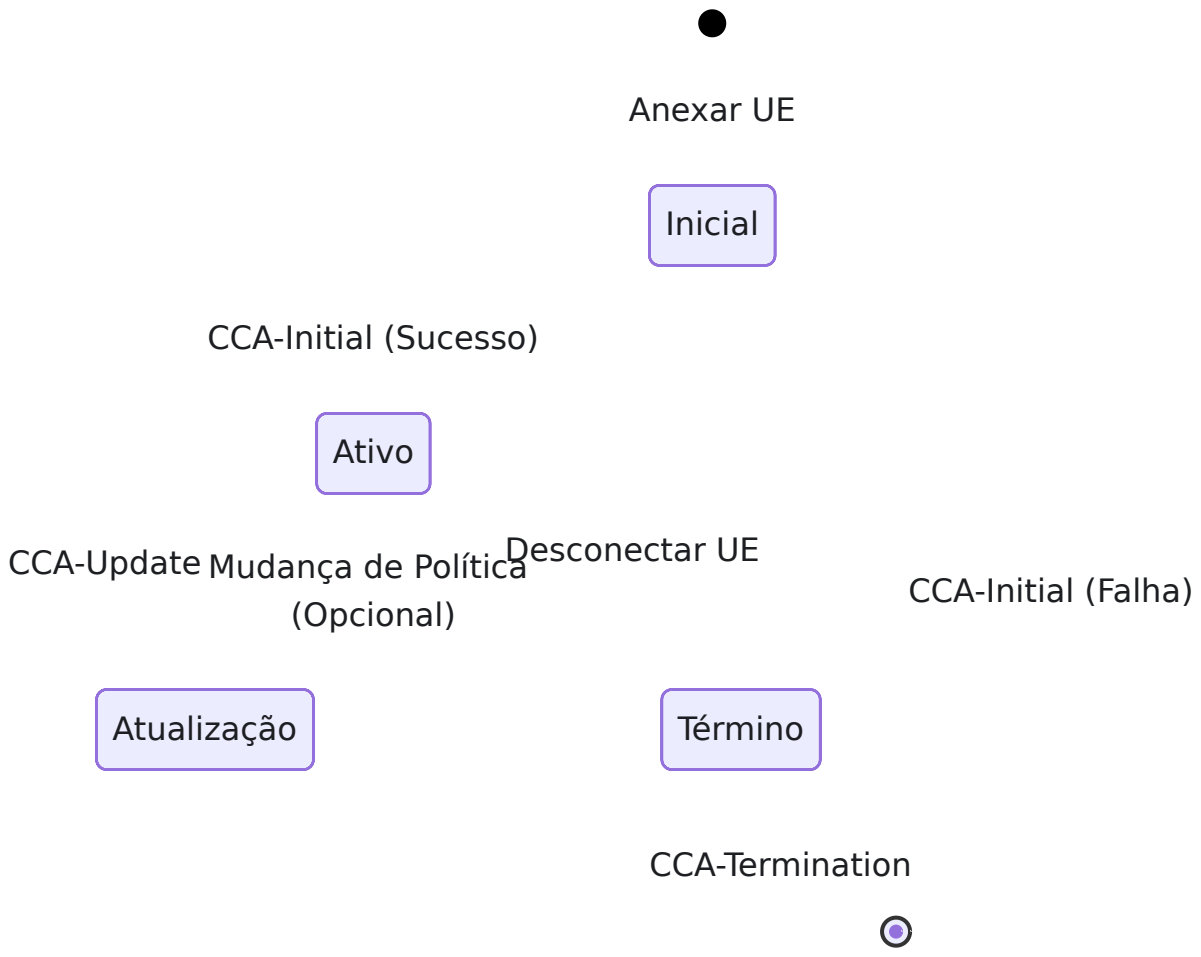
- `2001` - DIAMETER_SUCCESS
- `3xxx` - Erros de protocolo

- `4xxx` - Falhas transitórias
- `5xxx` - Falhas permanentes

Mensagens de Controle de Crédito

O PGW-C utiliza a **Aplicação de Controle de Crédito Diameter** (RFC 4006) para Gx.

Tipos de Mensagens



CCR-Initial (Requisição de Controle de Crédito - Inicial)

Quando: O UE cria uma nova conexão PDN

Propósito:

- Solicitar regras de política e cobrança iniciais
- Fornecer contexto do UE e da rede para a PCRF
- Obter parâmetros de QoS e autorização de cobrança

AVPs Chave Enviados pelo PGW-C:

Nome do AVP	Código do AVP	Tipo	Descrição
Session-Id	263	UTF8String	Identificador único da sessão Gx
Auth-Application-Id	258	Unsigned32	16777238 (Gx)
Origin-Host	264	DiamIdent	Identidade Diameter do PGW-C
Origin-Realm	296	DiamIdent	Reino Diameter do PGW-C
Destination-Realm	283	DiamIdent	Reino da PCRF
CC-Request-Type	416	Enumerated	1 = INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Número de sequência (começa em 0)
Subscription-Id	443	Grouped	Identificador do UE (IMSI/MSISDN)
Called-Station-Id	30	UTF8String	Nome da APN
Framed-IP-Address	8	OctetString	Endereço IPv4 alocado ao UE
IP-CAN-Type	1027	Enumerated	5 = 3GPP-EPS
RAT-Type	1032	Enumerated	1004 = EUTRAN
QoS-Information	1016	Grouped	QoS atual (AMBR)

Nome do AVP	Código do AVP	Tipo	Descrição
Network-Request-Support	1024	Enumerated	Procedimentos iniciados pela rede
Supported-Features	628	Grouped	Lista de recursos Gx

Exemplo de Estrutura CCR-I:

```
CCR (Código do Comando: 272, Requisição)
├── Session-Id: "pgw_c.example.com;123;456"
├── Auth-Application-Id: 16777238
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── Subscription-Id (Agrupado)
│   ├── Subscription-Id-Type: END_USER_IMSI (1)
│   └── Subscription-Id-Data: "310260123456789"
├── Called-Station-Id: "internet"
├── Framed-IP-Address: 100.64.1.42
├── IP-CAN-Type: 3GPP-EPS (5)
├── RAT-Type: EUTRAN (1004)
├── QoS-Information (Agrupado)
│   ├── APN-Aggregate-Max-Bitrate-UL: 100000000 (100 Mbps)
│   └── APN-Aggregate-Max-Bitrate-DL: 50000000 (50 Mbps)
├── Network-Request-Support: 1
└── Supported-Features: [...]
```

CCA-Initial (Resposta de Controle de Crédito - Inicial)

Enviado por: PCRF em resposta ao CCR-I

Propósito:

- Autorizar ou rejeitar a sessão
- Fornecer regras de PCC para manuseio de tráfego
- Especificar parâmetros de QoS

AVPs Chave Recebidos pelo PGW-C:

Nome do AVP	Código do AVP	Descrição
Result-Code	268	Sucesso (2001) ou código de erro
Experimental-Result	297	Códigos de resultado específicos do fornecedor
QoS-Information	1016	QoS autorizada (pode diferir da solicitação)
Charging-Rule-Install	1001	Regras de PCC a serem ativadas
Charging-Rule-Definition	1003	Definições de regras inline
Default-EPS-Bearer-QoS	1049	QoS para bearer padrão

Exemplo de Resposta de Sucesso:

```
CCA (Código do Comando: 272, Resposta)
├── Session-Id: "pgw_c.example.com;123;456"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "pcrf.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 16777238
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── QoS-Information (Agrupado)
│   ├── APN-Aggregate-Max-Bitrate-UL: 50000000 (50 Mbps -
reduzido)
│   └── APN-Aggregate-Max-Bitrate-DL: 100000000 (100 Mbps -
aumentado)
├── Charging-Rule-Install (Agrupado)
│   ├── Charging-Rule-Name: "default_internet_rule"
│   └── Charging-Rule-Name: "video_streaming_rule"
└── Charging-Rule-Definition (Agrupado)
    ├── Charging-Rule-Name: "default_internet_rule"
    ├── QoS-Information: {...}
    └── Precedence: 1000
```

CCR-Termination (Requisição de Controle de Crédito - Término)

Quando: O UE se desconecta ou a conexão PDN é excluída

Propósito:

- Notificar a PCRF sobre a terminação da sessão
- Registro final de contabilidade/cobrança

Diferenças Chave em Relação ao CCR-I:

- `CC-Request-Type: TERMINATION_REQUEST (3)`
- Pode incluir estatísticas de uso
- Conjunto de AVPs simplificado

Exemplo CCR-T:

```
CCR (Código do Comando: 272, Requisição)
├── Session-Id: "pgw_c.example.com;123;456"
├── Auth-Application-Id: 16777238
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: TERMINATION_REQUEST (3)
├── CC-Request-Number: 1
└── Termination-Cause: DIAMETER_LOGOUT (1)
```

CCA-Termination

Enviado por: PCRF em resposta ao CCR-T

Propósito:

- Reconhecer a terminação da sessão
- Nenhuma regra de política retornada

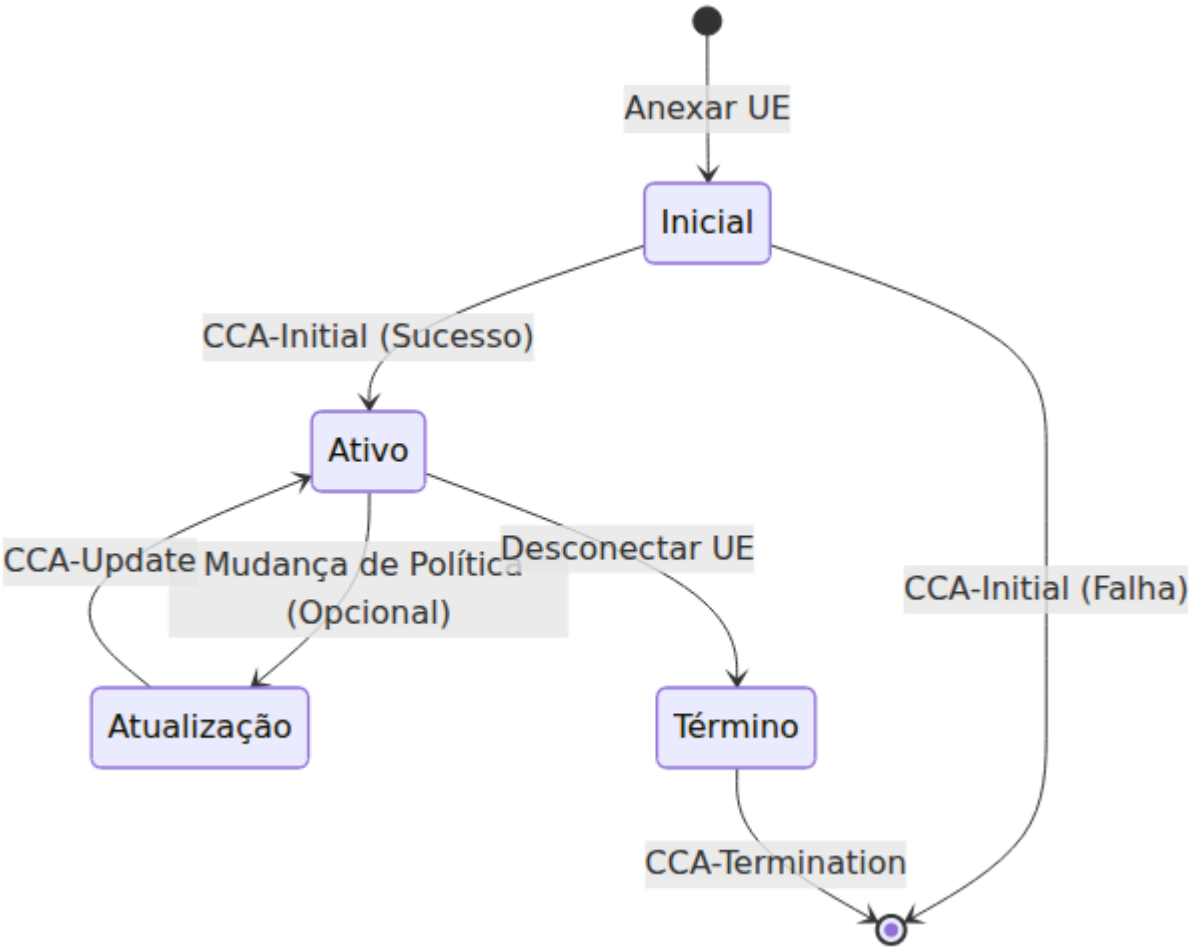
Exemplo CCA-T:

```
CCA (Código do Comando: 272, Resposta)
├── Session-Id: "pgw_c.example.com;123;456"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "pcrf.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 16777238
├── CC-Request-Type: TERMINATION_REQUEST (3)
└── CC-Request-Number: 1
```

Regras de Política e Cobrança

Estrutura da Regra PCC

Uma **Regra PCC (Controle de Política e Cobrança)** define como lidar com fluxos de tráfego específicos:



Componentes da Regra

1. Nome da Regra:

- Identificador único para a regra
- Exemplo: `"video_streaming_rule"`

2. Precedência:

- Número menor = maior prioridade
- Faixa: 0-65535
- Usado quando várias regras correspondem

3. Filtros de Fluxo (TFT - Modelo de Fluxo de Tráfego):

- Define quais pacotes correspondem a esta regra
- Exemplos:
  - IP 5-tuple: Protocolo, IP Src/Dst, Porta Src/Dst

- `"permit out ip from any to 8.8.8.8 80"`

4. Informações de QoS:

- **QCI (Identificador de Classe de QoS):** 1-9 (padronizado), 128-254 (específico do operador)
  - QCI 1: Voz Conversacional
  - QCI 5: Sinalização IMS
  - QCI 9: Internet Padrão
- **ARP (Prioridade de Alocação e Retenção):** Capacidade de preempção
- **MBR/GBR:** Taxas de Bits Máxima/Garantida

5. Informações de Cobrança:

- **Grupo de Tarifação:** Identifica a categoria de cobrança (usado pelo OCS - veja Interface Diameter Gy)
- **Método de Medição:** Baseado em volume, tempo ou evento
- **Cobrança Online/Offline:** OCS (pré-pago via Diameter Gy) vs. CDRs offline (pós-pago - veja Formato de CDR de Dados)

6. Status de Gating:

- **ABERTO:** Permitir tráfego
- **FECHADO:** Bloquear tráfego

Provisionamento Dinâmico de Regras

A PCRF pode fornecer regras de duas maneiras:

1. Regras Predefinidas (por nome):

```
Charging-Rule-Install (Agrupado)
├── Charging-Rule-Name: "gold_subscriber_internet"
└── Charging-Rule-Name: "video_qos_boost"
```

2. Regras Dinâmicas (definição inline):

```
Charging-Rule-Definition (Agrupado)
├── Charging-Rule-Name: "dynamic_rule_123"
├── Precedência: 100
├── Flow-Information (Agrupado)
│   ├── Flow-Description: "permit out ip from any to 192.0.2.0/24"
│   └── Flow-Direction: DOWNLINK
├── QoS-Information (Agrupado)
│   ├── QoS-Class-Identifier: 5
│   ├── Max-Requested-Bandwidth-UL: 10000000
│   └── Max-Requested-Bandwidth-DL: 50000000
└── Rating-Group: 1000
```

AVP de Informações de QoS

APN-AMBR (Taxa Máxima Agregada):

Aplica-se a todos os bearers não-GBR para esta APN:

```
QoS-Information (Agrupado)
├── APN-Aggregate-Max-Bitrate-UL: 100000000  # 100 Mbps
└── APN-Aggregate-Max-Bitrate-DL: 200000000  # 200 Mbps
```

Resposta do PGW-C:

- Atualiza o estado interno do AMBR
- Envia uma Solicitação de Modificação de Sessão para o PGW-U com o QER atualizado

---

Configuração

Configuração Básica do Gx

Edite `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    # Endereço IP para escutar conexões Diameter
    listen_ip: "0.0.0.0",

    # Identidade Diameter do PGW-C (Origin-Host)
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",

    # Reino Diameter do PGW-C (Origin-Realm)
    realm: "epc.mnc999.mcc999.3gppnetwork.org",

    # Lista de pares PCRF
    peer_list: [
      %{
        # Identidade Diameter da PCRF
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",

        # Reino da PCRF (geralmente o mesmo que o reino do PGW-C)
        realm: "epc.mnc999.mcc999.3gppnetwork.org",

        # Endereço IP da PCRF
        ip: "10.0.0.30",

        # Se o PGW-C inicia a conexão com a PCRF
        # true = PGW-C conecta-se à PCRF
        # false = Aguarda a PCRF se conectar
        initiate_connection: true
      }
    ]
  }
```

Múltiplos Pares PCRF

Para redundância ou distribuição geográfica:

```
config :pgw_c,
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf-primary.example.com",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.1.30",
        initiate_connection: true
      },
      %{
        host: "pcrf-backup.example.com",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.2.30",
        initiate_connection: true
      }
    ]
  }
```

Balanceamento de Carga:

- O protocolo Diameter lida com a seleção de pares
- Solicitações distribuídas com base na disponibilidade
- Failover automático em caso de falha do par

Resolução de Nome de Host

Identidades Diameter devem ser FQDNs (Nomes de Domínio Totalmente Qualificados):

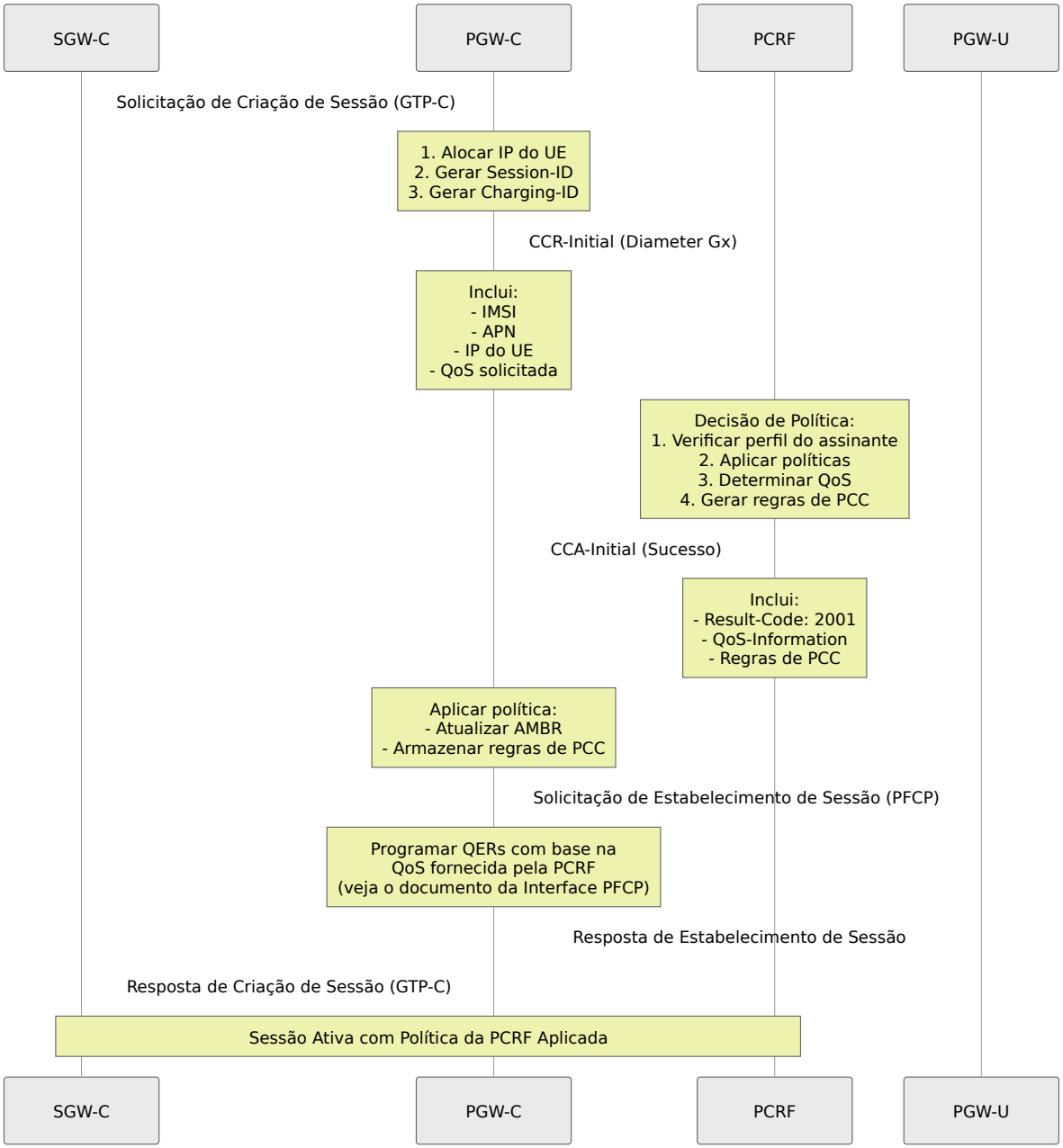
```
# CORRETO - formato FQDN
host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org"

# INCORRETO - Não é uma Identidade Diameter válida
host: "pgw_c"
host: "10.0.0.20"  # Endereços IP não são permitidos
```

Formato do Reino:

- Deve ser um nome de domínio válido
- Geralmente corresponde ao formato PLMN 3GPP: `epc.mncXXX.mccYYY.3gppnetwork.org`

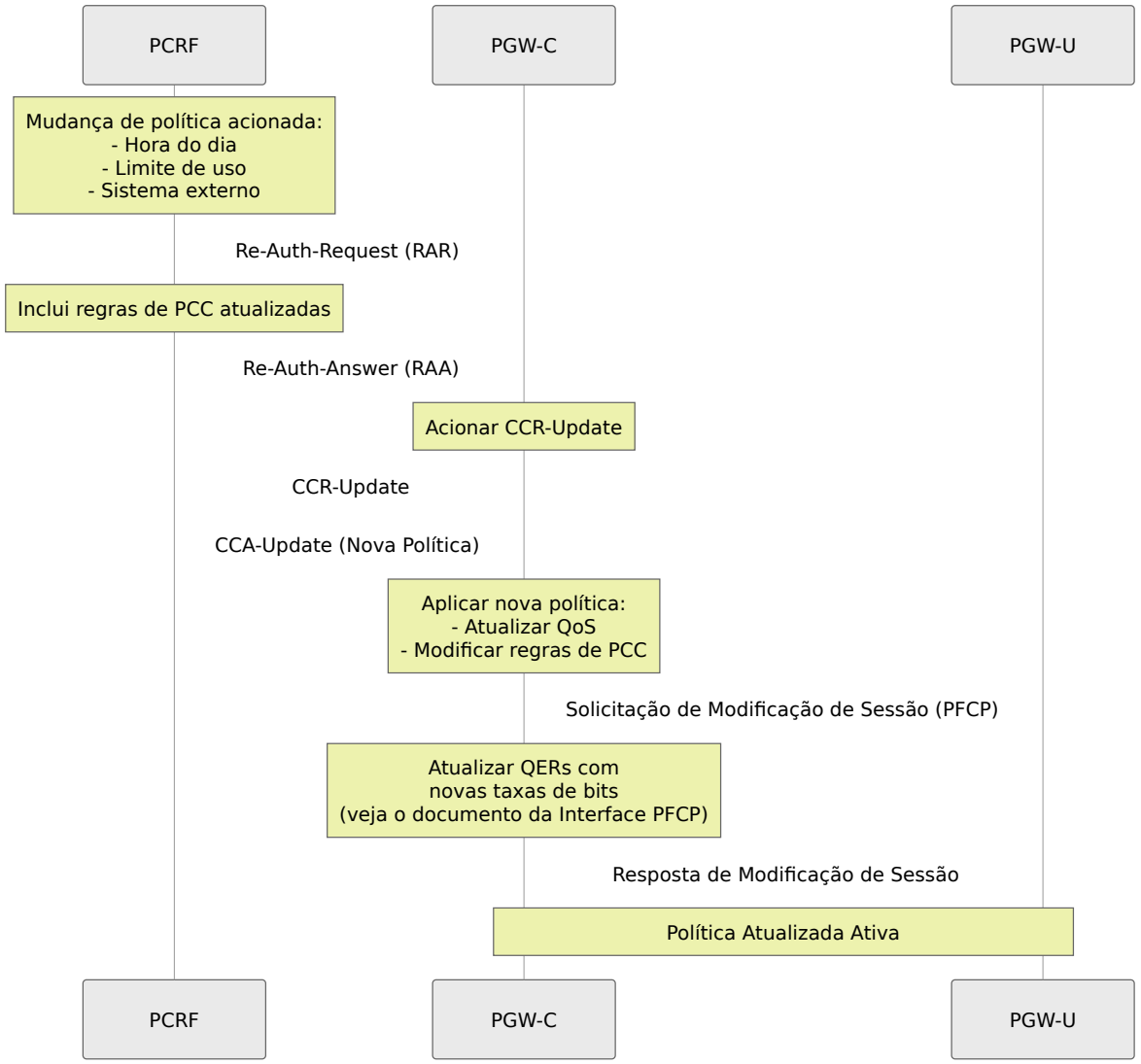
Fluxos de Mensagens

Estabelecimento de Sessão Bem-Sucedido

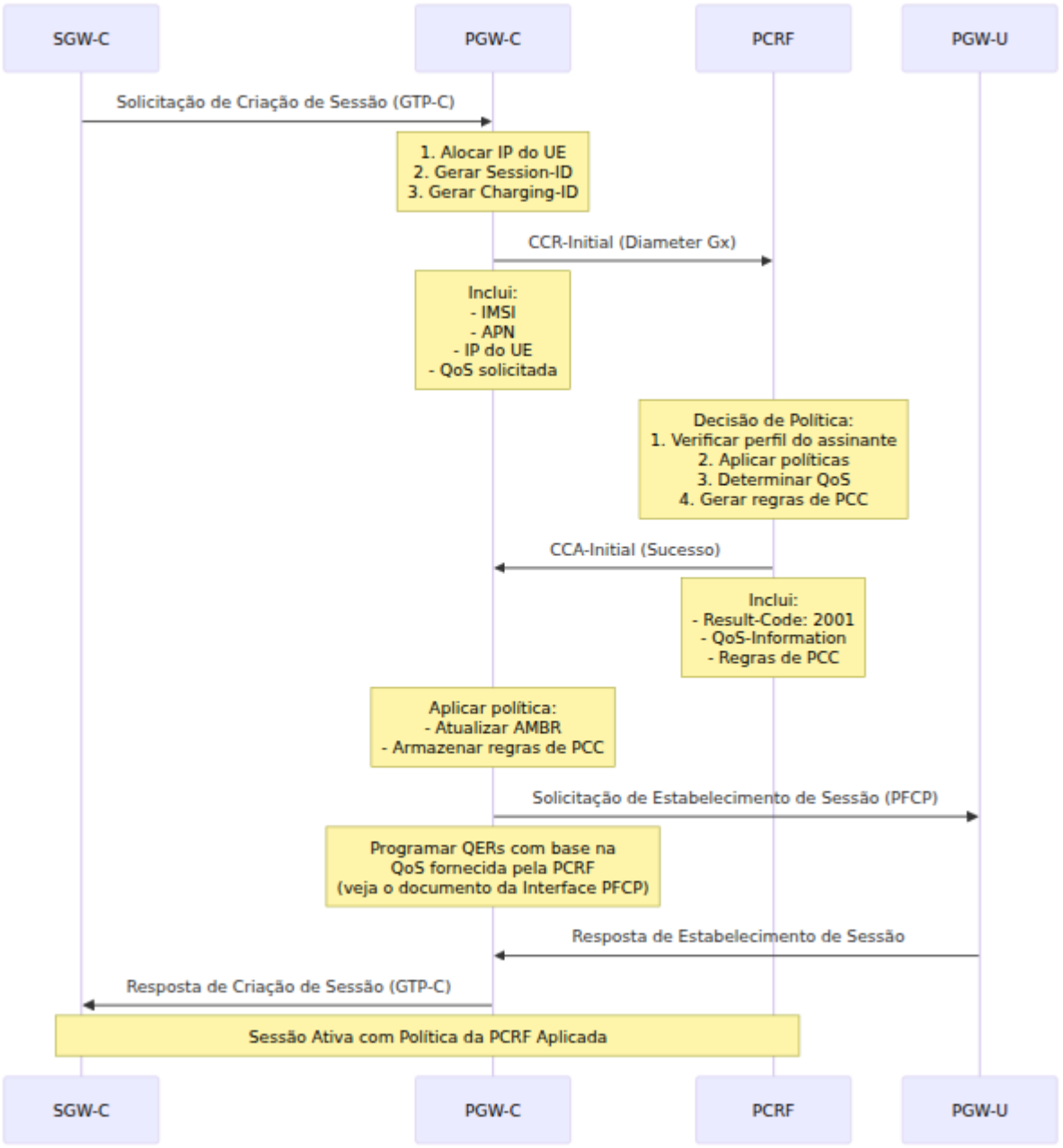


Nota: Os parâmetros de QoS da PCRF são traduzidos em QERs (Regras de Aplicação de QoS) e programados no PGW-U via PFCP. Veja Interface PFCP para detalhes sobre QER.

Atualização de Política (Iniciada pela Rede)



Término da Sessão



Tratamento de Erros

Códigos de Resultado

O PGW-C lida com vários códigos de resultado Diameter nas mensagens CCA:

Códigos de Sucesso:

Código	Nome	Ação
2001	DIAMETER_SUCCESS	Continuar o estabelecimento da sessão

Falhas Permanentes (5xxx):

Código	Nome	Ação do PGW-C
5002	DIAMETER_UNKNOWN_SESSION_ID	Registrar erro, falhar sessão
5030	DIAMETER_USER_UNKNOWN	Rejeitar sessão (Usuário Desconhecido)
5140	DIAMETER_ERROR_INITIAL_PARAMETERS	Registrar erro, tentar novamente ou falhar
5003	DIAMETER_AUTHORIZATION_REJECTED	Rejeitar sessão (Não Autorizado)

Falhas Transitórias (4xxx):

Código	Nome	Ação do PGW-C
4001	DIAMETER_AUTHENTICATION_REJECTED	Tentar novamente ou falhar sessão
4010	DIAMETER_TOO_BUSY	Tentar novamente com backoff
4012	DIAMETER_UNABLE_TO_COMPLY	Registrar erro, pode tentar novamente

Códigos de Resultado Experimentais

Códigos de erro específicos do fornecedor:

```
Experimental-Result (Agrupado)
├── Vendor-Id: 10415 (3GPP)
└── Experimental-Result-Code: <código específico do fornecedor>
```

Códigos Experimentais Comuns 3GPP:

Código	Nome	Significado
5065	IP_CAN_SESSION_NOT_AVAILABLE	PCRF não pode estabelecer sessão
5143	INVALID_SERVICE_INFORMATION	Dados de serviço inválidos

Tratamento de Timeouts

Timeout CCR-I:

Se a PCRF não responder ao CCR-Initial dentro do timeout:

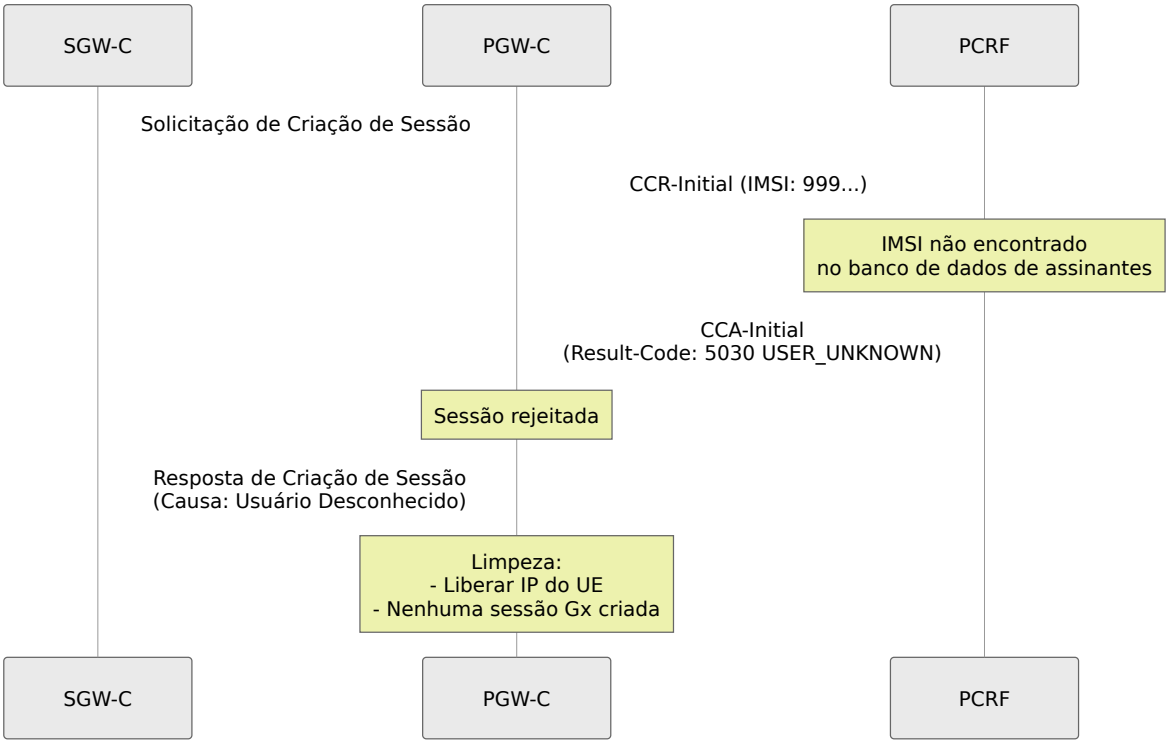
```
1. PGW-C aguarda o timeout configurado (por exemplo, 5 segundos)
2. Se nenhum CCA recebido:
   - Registrar: "timeout CCR-Initial para Session-ID: ..."
   - Responder ao SGW-C com causa de erro
   - Limpar recursos alocados
3. SGW-C recebe: Resposta de Criação de Sessão (Causa: Par Remoto
Não Respondendo)
```

Resposta de Erro ao SGW-C:

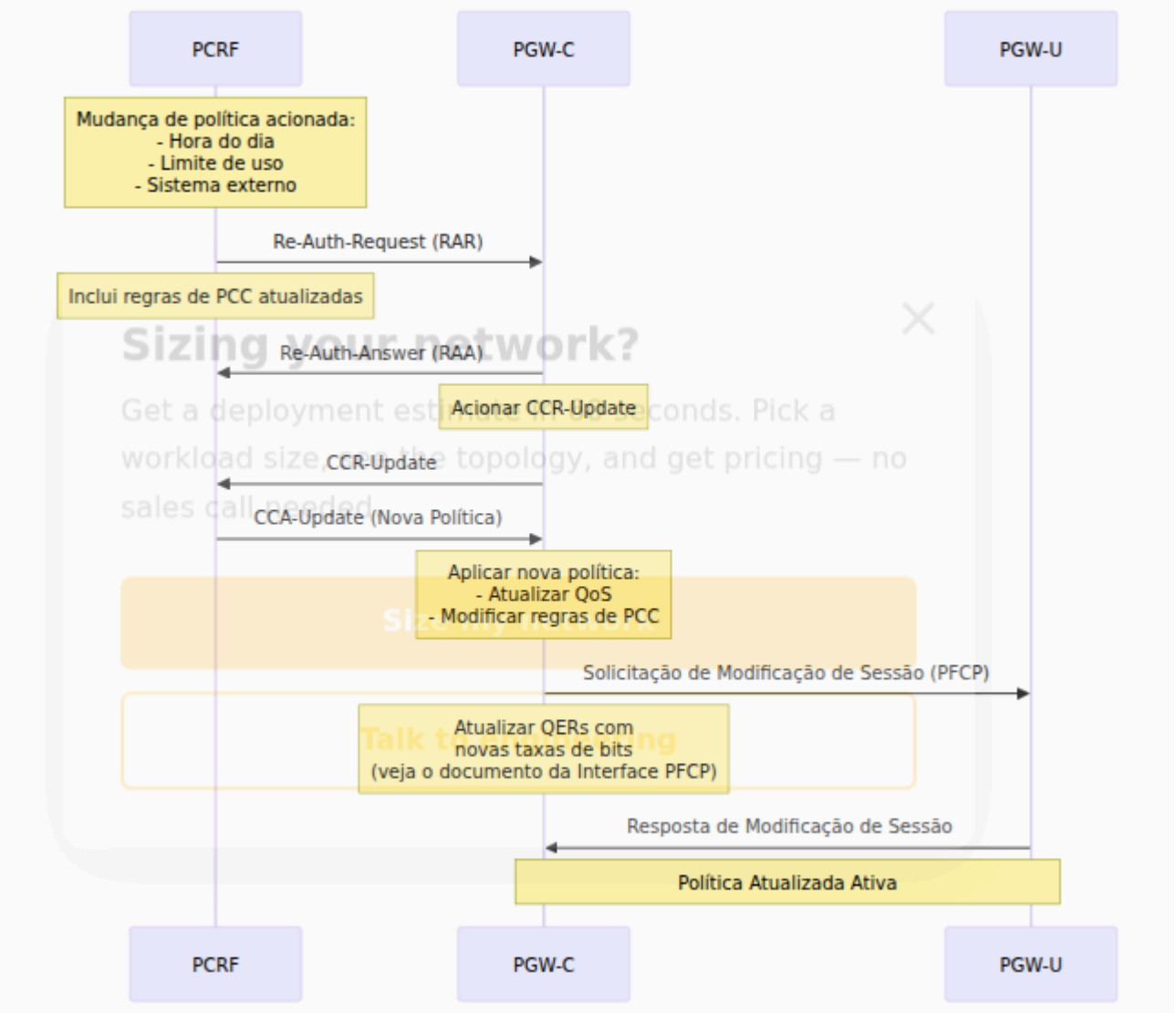
Quando o CCR-Initial expira, o PGW-C envia uma Resposta de Criação de Sessão com o código de causa `:remote_peer_not_responding` para o SGW-C.

Cenários de Falha

Cenário 1: PCRF Rejeita a Sessão (Usuário Desconhecido)



Cenário 2: PCRF Temporariamente Indisponível



Solução de Problemas

Problemas Comuns

1. Falha na Conexão do Par Diameter

Sintomas:

- Registro: "par Diameter não conectado"
- Nenhum CCR-Initial enviado

Causas Possíveis:

- PCRF não acessível
- IP da PCRF incorreto na configuração
- Firewall bloqueando a porta Diameter (3868)
- Identidades Diameter incorretas (host/reino)

Resolução:

```
# Testar conectividade de rede
ping <pcrf_ip>

# Testar porta Diameter (TCP 3868)
telnet <pcrf_ip> 3868

# Verificar configuração da identidade Diameter
# Garantir que host e reino sejam FQDNs, não IPs
```

Verificar Configuração:

```
config :pgw_c,
  diameter: %{
    # Deve ser FQDN, não IP
    host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.30"
      }
    ]
  }
```

2. Timeouts do CCR-Initial

Sintomas:

- Falha na Solicitação de Criação de Sessão
- Registro: "timeout CCR-Initial"

Causas Possíveis:

- PCRF sobrecarregada
- Latência de rede
- PCRF não respondendo a este Session-ID

Resolução:

1. Verificar logs da PCRF para erros
2. Confirmar que a PCRF está processando solicitações
3. Verificar latência de rede: `ping <pcrf_ip>`
4. Aumentar o timeout se a latência da rede for alta

3. Sessões Rejeitadas pela PCRF

Sintomas:

- CCA-Initial com Result-Code != 2001
- Falha na Resposta de Criação de Sessão

Códigos de Resultado Comuns:

Código de Resultado	Causa Provável	Resolução
5030	IMSI não no banco de dados de assinantes	Provisionar assinante no HSS/SPR
5003	Autorização rejeitada	Verificar permissões do assinante
4010	PCRF muito ocupada	Tentar novamente ou aumentar a capacidade da PCRF

Verificar Logs:

```
# Logs do PGW-C mostram:
[error] Erro Diameter Gx: Código de Resultado 5030
(DIAMETER_USER_UNKNOWN)
[error] IMSI 310260999999999 rejeitado pela PCRF
```

4. QoS Não Aplicada

Sintomas:

- Sessão estabelecida, mas QoS incorreta
- Taxas de bits não correspondem aos valores esperados

Etapas de Depuração:

1. **Verificar CCA-Initial:**
    - Confirmar que o AVP `QoS-Information` está presente
    - Verificar os valores de `APN-Aggregate-Max-Bitrate-UL/DL`
2. **Verificar Estabelecimento da Sessão PFCP:**
    - Confirmar que QER foi criado com os valores corretos de MBR
    - Verificar logs do PGW-U para instalação de QER
3. **Verificar Política da PCRF:**
    - Verificar configuração da PCRF
    - Confirmar que o perfil do assinante inclui QoS correta

5. Problemas de Roteamento Diameter

Sintomas:

- Mensagens Diameter não chegam à PCRF
- Registro: "Sem rota para Destination-Realm"

Causa:

- Desvio de reino entre configuração e mensagens

Resolução:

Garantir consistência:

```
# Todos devem corresponder
config :pgw_c,
  diameter: %{
    realm: "epc.mnc999.mcc999.3gppnetwork.org",  # Reino do PGW-C
    peer_list: [
      %{
        realm: "epc.mnc999.mcc999.3gppnetwork.org"  # Reino da
PCRF (geralmente o mesmo)
      }
    ]
  }
```

No CCR-Initial:

```
Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
```

Monitoramento da Saúde do Gx

Métricas Chave:

```
# Taxas de mensagens Gx
rate(gx_inbound_messages_total{message_type="gx_CCA"}[5m])
rate(gx_outbound_messages_total{message_type="gx_CCR"}[5m])

# Taxas de erro do Gx
rate(gx_inbound_errors_total[5m])

# Taxa de sucesso de respostas do Gx (nova métrica)
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Falhas de resposta do Gx por host PCRF
rate(gx_outbound_responses_total{result_code_class!="2xxx"}[5m])
by (diameter_host)

# Contagem de sessões do Gx
session_id_registry_count

# Duração do manuseio de mensagens do Gx
histogram_quantile(0.95,
rate(gx_inbound_handling_duration_bucket[5m]))
```

Métricas de Resposta por Classe de Código de Resultado:

A métrica `gx_outbound_responses_total` fornece visibilidade detalhada sobre as respostas Diameter enviadas para pares PCRF, categorizadas por:

- **`message_type`**: Tipo de mensagem de resposta (`gx_RAA`, `gx_CCA`)
- **`result_code_class`**: Categoria de código de resultado (`2xxx`, `3xxx`, `4xxx`, `5xxx`)
- **`diameter_host`**: Par PCRF recebendo a resposta

Códigos de Resultado Comuns:

- **2001** (DIAMETER_SUCCESS) - Resposta bem-sucedida
- **3001** (DIAMETER_COMMAND_UNSUPPORTED) - Erro de protocolo
- **5012** (DIAMETER_UNABLE_TO_COMPLY) - Não pode executar a solicitação
- **5030** (DIAMETER_USER_UNKNOWN) - Assinante não encontrado

Exemplos de Alertas:

```
# Alerta sobre alta taxa de erro do Gx
- alert: GxErrorRateHigh
  expr: rate(gx_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Alta taxa de erro do Gx detectada"

# Alerta sobre alta taxa de falha de resposta do Gx
- alert: GxResponseFailureRate
  expr: |

sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
    sum(rate(gx_outbound_responses_total[5m])) > 0.1
  for: 5m
  annotations:
    summary: "Alta taxa de falha de resposta do Gx"
    description: "Mais de 10% das respostas do Gx são falhas"

# Alerta sobre rejeição de sessão
- alert: GxSessionRejection
  expr: rate(gx_inbound_errors_total{result_code="5030"}[5m]) >
0.01
  for: 5m
  annotations:
    summary: "PCRF rejeitando sessões (USER_UNKNOWN)"
```

Registro de Depuração

Habilitar registro verbose do Diameter:

```
# config/runtime.exs
config :logger, level: :debug

# Ou em tempo de execução
iex> Logger.configure(level: :debug)
```

Procurar por:

- `[debug] Enviando CCR-Initial para Session-ID: ...`
- `[debug] Recebido CCA-Initial: Result-Code 2001`
- `[error] Erro Diameter: ...`

Interface Web - Monitoramento de Pares Diameter

O OmniPGW inclui uma interface Web em tempo real para monitorar conexões e status de pares Diameter.

Página de Pares Diameter

Acesso: `http://<omnipgw-ip>:<web-port>/diameter`

Propósito: Monitorar a conectividade do par Diameter Gx com a PCRF em tempo real

Recursos:

1. Visão Geral da Conexão do Par

- **Contagem Conectada** - Número de pares PCRF com conexão ativa
- **Contagem Desconectada** - Número de pares configurados, mas não conectados
- Atualiza automaticamente a cada 1 segundo (a atualização mais rápida de todas as páginas)

2. Informações de Status por Par Para cada par PCRF configurado:

- **Host** - Identidade Diameter (Origin-Host)
- **Endereço IP** - IP da PCRF
- **Porta** - Porta Diameter (padrão 3868)
- **Status** - Conectado (verde) / Desconectado (vermelho)
- **Transporte** - TCP ou SCTP
- **Iniciação da Conexão** - Quem inicia (PGW ou PCRF)
- **Reino** - Reino Diameter
- **Nome do Produto** - Identificador do produto PCRF (se anunciado)
- **IDs de Aplicação** - Aplicações Diameter suportadas (por exemplo, Gx = 16777238)

3. Detalhes Expansíveis Clique em qualquer linha de par para ver:

- Configuração completa do par
- Detalhes da Troca de Capacidades (CER/CEA)
- Recursos suportados
- Estado completo da conexão

Casos de Uso Operacionais

Monitorar Conectividade da PCRF:

```
1. Abra a página Diameter no navegador
2. Verifique se todos os pares PCRF mostram "Conectado"
3. Verifique se a Iniciação da Conexão corresponde à configuração
4. Verifique se os IDs de Aplicação incluem Gx (16777238)
```

Solução de Problemas de Falhas na Criação de Sessões (Problemas Gx):

```
1. Sessões de usuários falhando com erros "timeout PCRF"
2. Abra a página Diameter
3. Verifique o status do par:
   - Desconectado?
     → Verifique a conectividade de rede
     → Confirme que a PCRF está em execução
     → Verifique regras de firewall para TCP 3868
   - Conectado, mas sessões falhando?
     → O problema está no nível da aplicação (verifique logs)
     → A PCRF pode estar rejeitando assinantes
```

Verificar Configuração Diameter:

```
1. Após configurar um novo par PCRF
2. Abra a página Diameter
3. Verifique se o par aparece na lista
4. Verifique se o status muda para "Conectado"
5. Expanda o par para verificar:
   - Reino corresponde à configuração
   - IDs de Aplicação incluem Gx
   - Nome do Produto mostra identificador da PCRF
```

Monitorar Failover:

```
Cenário: PCRF primária falha
1. A página Diameter mostra primária "Desconectada"
2. Verifique se a PCRF de backup ainda está "Conectada"
3. Novas sessões usam automaticamente o backup
4. Quando a primária se recupera, o status retorna a "Conectado"
```

Detectar Problemas de Roteamento Diameter:

- O par mostra "Conectado", mas reino errado
- IDs de Aplicação não incluem Gx (16777238)
- Nome do Produto não corresponde à PCRF esperada

Identificar Inconsistências de Configuração:

```
A interface Web mostra:
  Iniciação da Conexão: "O par inicia"
Mas a configuração diz:
  initiate_connection: true

Isso indica:
  - OmniPGW tenta se conectar
  - Mas a PCRF também está iniciando
  - Pode causar condições de corrida de conexão
```

Vantagens:

- **Taxa de atualização mais rápida** - Atualizações a cada 1 segundo
- **Status de conexão visual** - Indicação imediata em vermelho/verde
- **Sem ferramentas Diameter necessárias** - Sem necessidade de ferramentas CLI diameter
- **Configuração do par visível** - Verificar configurações sem verificar arquivos de configuração
- **Detalhes em nível de aplicação** - Ver recursos Diameter suportados
- **Verificação de reino** - Confirmar configuração de roteamento Diameter

Integração com Métricas

Enquanto a interface Web fornece status em tempo real, combine com Prometheus para:

- Taxas de erro históricas do Gx
- Contagens de mensagens CCR/CCA
- Tendências de latência

Interface Web = "Está funcionando agora?" Métricas = "Como tem funcionado ao longo do tempo?"

Documentação Relacionada

Configuração e Política

- **Guia de Configuração** - Configuração Diameter, configuração de pares PCRF
- **Interface PFCP** - Aplicação de QoS via QERs de regras de PCC
- **Gerenciamento de Sessão** - Ciclo de vida da sessão com integração de política
- **QoS & Gerenciamento de Bearer** - Configuração detalhada de QoS e configuração de bearer

Integração de Cobrança

- **Interface Diameter Gy** - Cobrança online acionada por regras de PCC
- **Formato de CDR de Dados** - Registros de cobrança offline com informações de política
- **Configuração PCO** - Entrega P-CSCF para controle de política IMS

Operações

- **Guia de Monitoramento** - Métricas do Gx, rastreamento de políticas, alertas de conectividade da PCRF
- **Interface S5/S8** - Integração de gerenciamento de bearer com política

---

Voltar ao Guia de Operações

Cobrança Online Diameter (Interface Gy/Ro)

Interface do Sistema de Cobrança Online (OCS)

Índice

Visão Geral

A **interface Gy** (também chamada de **interface Ro** em contextos IMS) conecta o PGW-C ao **Sistema de Cobrança Online (OCS)** para controle de crédito em tempo real. Isso permite:

- **Cobrança Pré-paga** - Autorização e dedução de crédito em tempo real

- **Controle de Crédito em Tempo Real** - Conceder cota antes da entrega do serviço
- **Cobrança Baseada em Serviço** - Cobrança diferente para voz, dados, SMS, etc.
- **Atualizações Imediatas de Conta** - Atualizações de saldo de crédito em tempo real
- **Negação de Serviço** - Bloquear serviço quando o crédito se esgotar

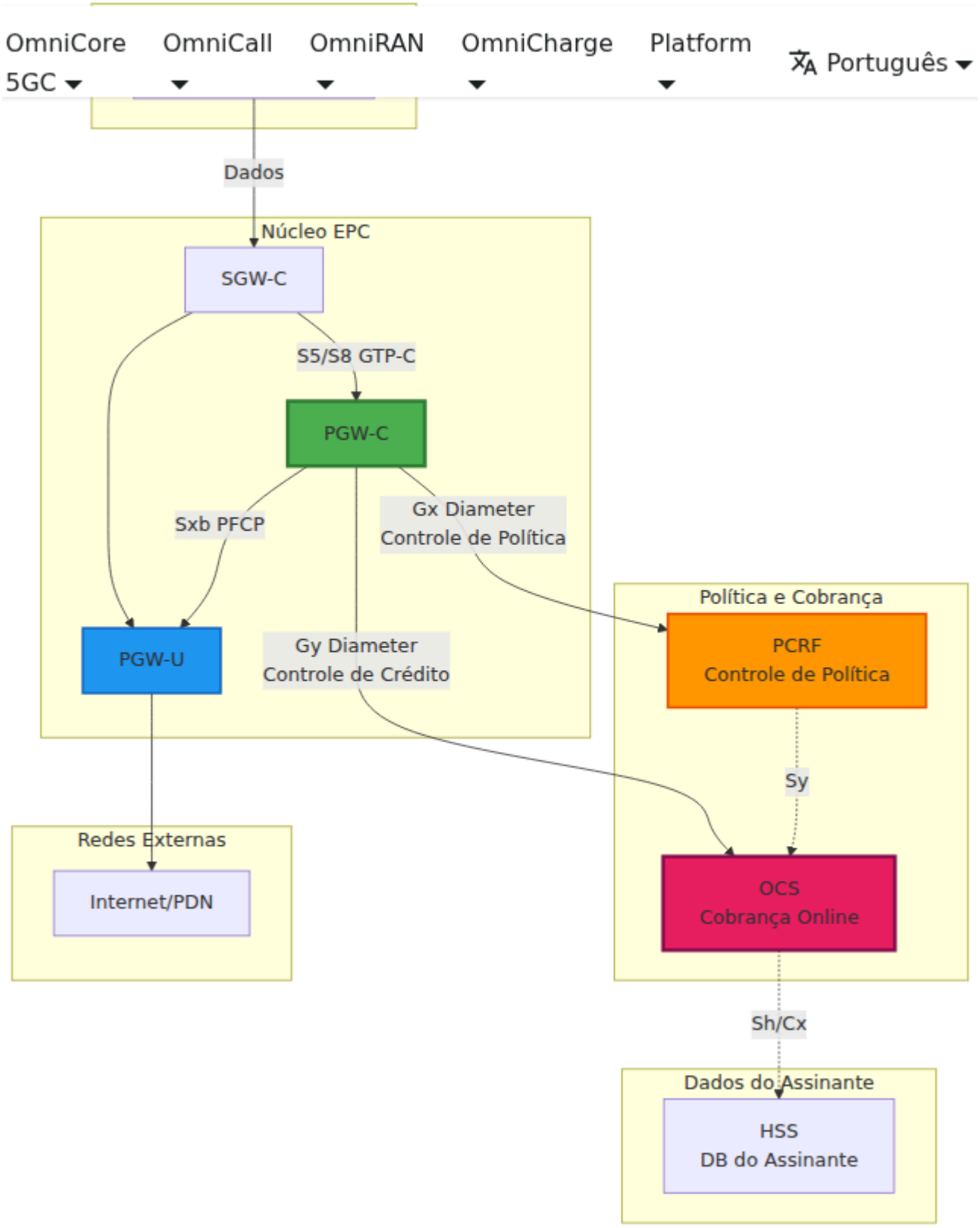
Cobrança Online vs. Offline

Aspecto	Cobrança Online (Gy/Ro)	Cobrança Offline (Gz/Rf)
Tempo	Em tempo real, antes do serviço	Após a entrega do serviço
Caso de Uso	Assinantes pré-pagos	Assinantes pós-pagos
Verificação de Crédito	Sim, antes de conceder o serviço	Não, fatura gerada posteriormente
Sistema	OCS (Sistema de Cobrança Online)	CGF/CDF (Função de Dados de Cobrança)
Risco	Sem perda de receita	Risco de faturas não pagas
Complexidade	Alta (requisitos em tempo real)	Menor (processamento em lote)
Impacto no Usuário	Serviço negado se não houver crédito	Serviço sempre disponível

Veja também: Formato CDR de Dados para registros de cobrança offline (faturamento pós-pago)

Veja também: Gerenciamento de Sessão para o ciclo de vida completo da sessão PDN, incluindo integração de cobrança

Gy na Arquitetura da Rede

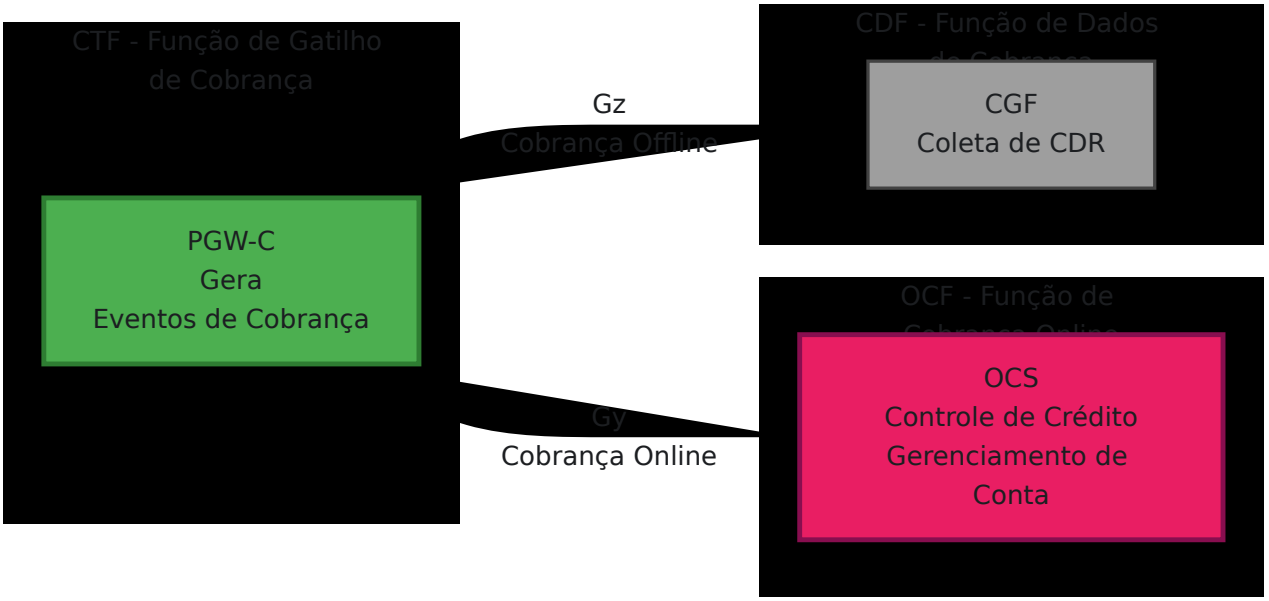


Funções Principais

Função	Descrição
Autorização de Crédito	Solicitar cota do OCS antes de permitir tráfego
Gerenciamento de Cota	Rastrear unidades concedidas (bytes, tempo, eventos)
Detecção de Esgotamento de Crédito	Monitorar cota restante
Reautorização	Solicitar cota adicional quando o limite for atingido
Término de Serviço	Parar o serviço quando o crédito se esgotar
Liquidação Final	Relatar uso real ao final da sessão

Arquitetura de Cobrança 3GPP

Pontos de Referência de Cobrança



Função de Gatilho de Cobrança (CTF)

O PGW-C atua como um **CTF (Função de Gatilho de Cobrança)**, responsável por:

1. **Detectar eventos cobrados** - Início da sessão, uso de dados, término da sessão
2. **Solicitar autorização de crédito** - Antes de permitir o serviço
3. **Rastrear consumo de cota** - Monitorar unidades concedidas
4. **Gerar eventos de cobrança** - Acionar solicitações de crédito
5. **Impor controle de crédito** - Bloquear tráfego quando a cota se esgotar

Função de Cobrança Online (OCF)

O OCS implementa a **OCF (Função de Cobrança Online)**:

1. **Gerenciamento de saldo de conta** - Rastrear crédito do assinante
2. **Classificação** - Determinar preço por unidade (por MB, por segundo, etc.)
3. **Reserva de crédito** - Reservar crédito para cota concedida

4. **Dedução de crédito** - Deduzir ao relatar uso
5. **Decisões de política** - Conceder ou negar com base no saldo

---

Fundamentos da Interface Gy/Ro

Referência 3GPP

- **Especificação:** 3GPP TS 32.299 (Arquitetura de cobrança)
- **Protocolo:** 3GPP TS 32.251 (Cobrança de domínio PS)
- **ID da Aplicação Diameter:** 4 (Gy/Ro - Aplicação de Controle de Crédito)
- **Protocolo Base:** RFC 4006 (Aplicação de Controle de Crédito Diameter)

Conceito de Sessão

Cada conexão PDN do UE que requer cobrança online tem uma **sessão Gy/Ro** identificada por um **Session-ID**. Esta sessão:

- Criada quando o bearer requer cobrança online (CCR-Initial)
- Atualizada quando a cota é consumida (CCR-Update)
- Terminada quando a sessão termina (CCR-Termination)

Formato do ID da Sessão

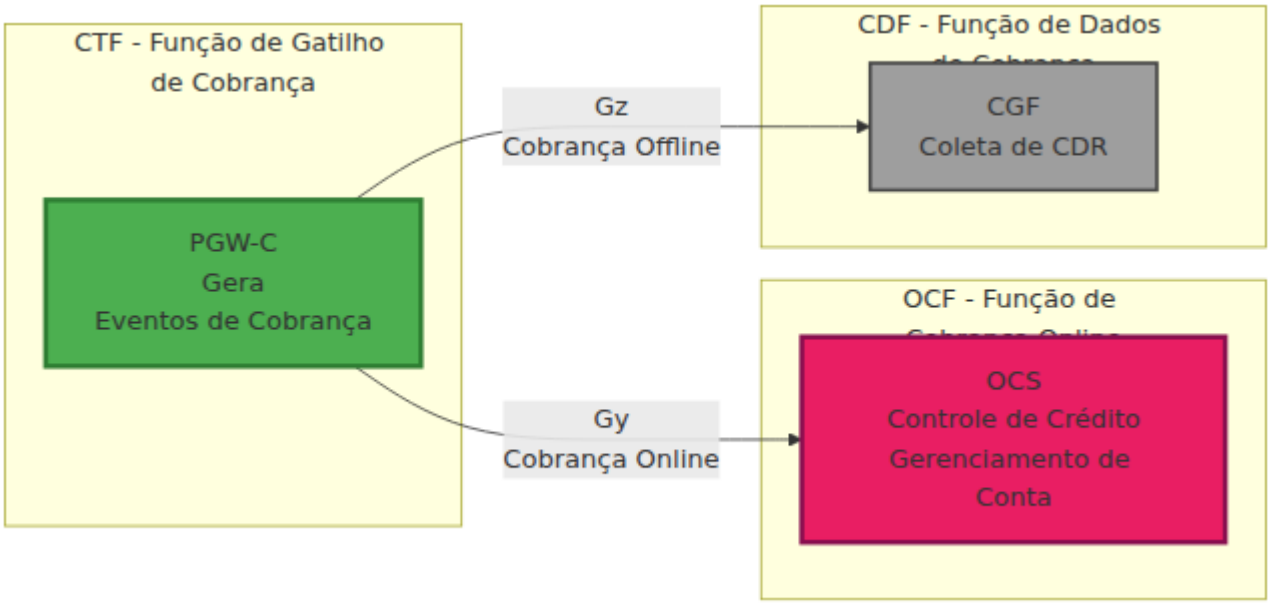
```
Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]
Exemplo: omni-
pgw_c.epc.mnc999.mcc999.3gppnetwork.org;9876543210;12345;gy
```

Componentes:

- **Origin-Host:** Identidade Diameter do PGW-C
- **high32:** 32 bits altos do identificador único
- **low32:** 32 bits baixos do identificador único
- **optional:** Identificador adicional (por exemplo, "gy" para distinguir do Gx)

Mensagens de Controle de Crédito

Tipos de Mensagens



CCR-Initial (Solicitação de Controle de Crédito - Inicial)

Quando: O UE cria uma conexão PDN e o bearer requer cobrança online

Propósito:

- Solicitar autorização de crédito inicial do OCS
- Reservar cota para entrega do serviço
- Estabelecer sessão Gy/Ro

Principais AVPs Enviados pelo PGW-C:

Nome do AVP	Código do AVP	Tipo	Descrição
Session-Id	263	UTF8String	Identificador único da sessão Gy
Auth-Application-Id	258	Unsigned32	4 (Controle de Crédito)
Origin-Host	264	DiamIdent	Identidade Diameter do PGW-C
Origin-Realm	296	DiamIdent	Reino Diameter do PGW-C
Destination-Realm	283	DiamIdent	Reino do OCS
CC-Request-Type	416	Enumerated	1 = INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Número da sequência (começa em 0)
Subscription-Id	443	Grouped	Identificador do UE (IMSI/MSISDN)
Service-Context-Id	461	UTF8String	Identificador do contexto de cobrança
Multiple-Services-Credit-Control	456	Grouped	Solicitações de crédito específicas do serviço
Requested-Service-Unit	437	Grouped	Cota solicitada (bytes, tempo, etc.)
Used-Service-Unit	446	Grouped	Cota usada (0 para inicial)

Nome do AVP	Código do AVP	Tipo	Descrição
Service-Identifier	439	Unsigned32	Identificador do tipo de serviço
Rating-Group	432	Unsigned32	Identificador da categoria de cobrança

Exemplo de Estrutura CCR-I:

```
CCR (Código do Comando: 272, Solicitação)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
├── Subscription-Id (Grouped)
│   ├── Subscription-Id-Type: END_USER_IMSI (1)
│   └── Subscription-Id-Data: "310260123456789"
├── Subscription-Id (Grouped)
│   ├── Subscription-Id-Type: END_USER_E164 (0)
│   └── Subscription-Id-Data: "15551234567"
├── Service-Context-Id: "32251@3gpp.org"
├── Multiple-Services-Credit-Control (Grouped)
│   ├── Service-Identifier: 1
│   ├── Rating-Group: 100
│   └── Requested-Service-Unit (Grouped)
│       └── CC-Total-Octets: 10000000 (solicitar 10 MB)
└── Used-Service-Unit (Grouped)
    └── CC-Total-Octets: 0 (sem uso ainda)
```

CCA-Initial (Resposta de Controle de Crédito - Inicial)

Enviado por: OCS em resposta ao CCR-I

Propósito:

- Conceder ou negar autorização de crédito
- Fornecer cota para entrega do serviço
- Especificar parâmetros de classificação e cobrança

Principais AVPs Recebidos pelo PGW-C:

Nome do AVP	Código do AVP	Descrição
Result-Code	268	Sucesso (2001) ou código de erro
Multiple-Services-Credit-Control	456	Concessões de crédito específicas do serviço
Granted-Service-Unit	431	Cota concedida (bytes, tempo, etc.)
Validity-Time	448	Período de validade da cota (segundos)
Result-Code	268	Código de resultado por serviço
Final-Unit-Indication	430	Ação quando a cota se esgotar
Volume-Quota-Threshold	-	Limite para reautorização

Exemplo de Resposta de Sucesso:

```
CCA (Código do Comando: 272, Resposta)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "ocs.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 4
├── CC-Request-Type: INITIAL_REQUEST (1)
├── CC-Request-Number: 0
└── Multiple-Services-Credit-Control (Grouped)
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    ├── Granted-Service-Unit (Grouped)
    │   └── CC-Total-Octets: 10000000 (concedido 10 MB)
    ├── Validity-Time: 3600 (cota válida por 1 hora)
    └── Volume-Quota-Threshold: 8000000 (re-autorização em 8 MB
usados, 80%)
```

CCR-Update (Solicitação de Controle de Crédito - Atualização)

Quando:

- Limite de cota concedida alcançado (por exemplo, 80% consumido)
- Tempo de validade expira
- Mudança de serviço requer reautorização
- Mudança de horário tarifário

Propósito:

- Solicitar cota adicional
- Relatar uso da cota previamente concedida
- Atualizar parâmetros de cobrança

Principais Diferenças em Relação ao CCR-I:

- `CC-Request-Type: UPDATE_REQUEST (2)`
- `CC-Request-Number` incrementado

- `Used-Service-Unit` contém uso real
- `Requested-Service-Unit` para mais cota

Exemplo de Estrutura CCR-U:

```
CCR (Código do Comando: 272, Solicitação)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: UPDATE_REQUEST (2)
├── CC-Request-Number: 1
└── Multiple-Services-Credit-Control (Grouped)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    ├── Used-Service-Unit (Grouped)
    │   └── CC-Total-Octets: 8000000 (8 MB usados até agora)
    └── Requested-Service-Unit (Grouped)
        └── CC-Total-Octets: 10000000 (solicitar mais 10 MB)
```

CCA-Update (Resposta de Controle de Crédito - Atualização)

Enviado por: OCS em resposta ao CCR-U

Propósito:

- Conceder cota adicional (se crédito disponível)
- Reconhecer uso
- Atualizar parâmetros de cobrança

Possíveis Resultados:

1. Mais Cota Concedida:

```
CCA (Atualização)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 10000000 (mais 10 MB)
    └── Validity-Time: 3600
```

2. Cota Final (Crédito Esgotado):

```
CCA (Atualização)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 1000000 (apenas 1 MB restante)
    └── Final-Unit-Indication
        └── Final-Unit-Action: TERMINATE (0)
```

3. Sem Crédito Disponível:

```
CCA (Atualização)
├── Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
    └── Final-Unit-Indication
        └── Final-Unit-Action: TERMINATE (0)
```

CCR-Termination (Solicitação de Controle de Crédito - Término)

Quando:

- UE se desanexa
- Conexão PDN excluída
- Sessão encerrada por qualquer motivo

Propósito:

- Relatório final de uso
- Fechar sessão Gy/Ro
- Liquidação final

Principais Diferenças:

- `CC-Request-Type: TERMINATION_REQUEST (3)`
- `Used-Service-Unit` contém uso final
- Sem `Requested-Service-Unit` (não é mais necessária cota)
- Inclui `Termination-Cause`

Exemplo de Estrutura CCR-T:

```
CCR (Código do Comando: 272, Solicitação)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Auth-Application-Id: 4
├── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
├── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
├── CC-Request-Type: TERMINATION_REQUEST (3)
├── CC-Request-Number: 5
├── Termination-Cause: DIAMETER_LOGOUT (1)
└── Multiple-Services-Credit-Control (Grouped)
    ├── Service-Identifier: 1
    ├── Rating-Group: 100
    └── Used-Service-Unit (Grouped)
        └── CC-Total-Octets: 18500000 (18.5 MB de uso total)
```

CCA-Termination (Resposta de Controle de Crédito - Término)

Enviado por: OCS em resposta ao CCR-T

Propósito:

- Reconhecer término da sessão
- Completar contabilidade
- Liberar crédito reservado

Exemplo CCA-T:

```
CCA (Código do Comando: 272, Resposta)
├── Session-Id: "pgw_c.example.com;123;456;gy"
├── Result-Code: DIAMETER_SUCCESS (2001)
├── Origin-Host: "ocs.example.com"
├── Origin-Realm: "example.com"
├── Auth-Application-Id: 4
├── CC-Request-Type: TERMINATION_REQUEST (3)
└── CC-Request-Number: 5
```

Fluxos de Cobrança Online

Tipos de Unidades de Serviço

O OCS pode conceder cota em diferentes unidades:

Tipo de Unidade	AVP	Descrição	Caso de Uso
Tempo	CC-Time	Segundos	Chamadas de voz, duração da sessão
Volume	CC-Total-Octets	Bytes (total up+down)	Serviços de dados
Volume (separado)	CC-Input-Octets, CC-Output-Octets	Bytes (separados)	Cobrança assimétrica
Específico do Serviço	CC-Service-Specific-Units	Unidades personalizadas	SMS, MMS, chamadas de API
Eventos	-	Eventos contados	Serviços pay-per-use

Gerenciamento de Limite de Cota

Problema: Como o PGW-C sabe quando solicitar mais cota?

Solução: O OCS fornece um **Volume-Quota-Threshold** ou **Time-Quota-Threshold**. O PGW-C monitora o uso via Relatórios de Sessão PFCP do PGW-U (veja Interface PFCP).

Exemplo de Fluxo:

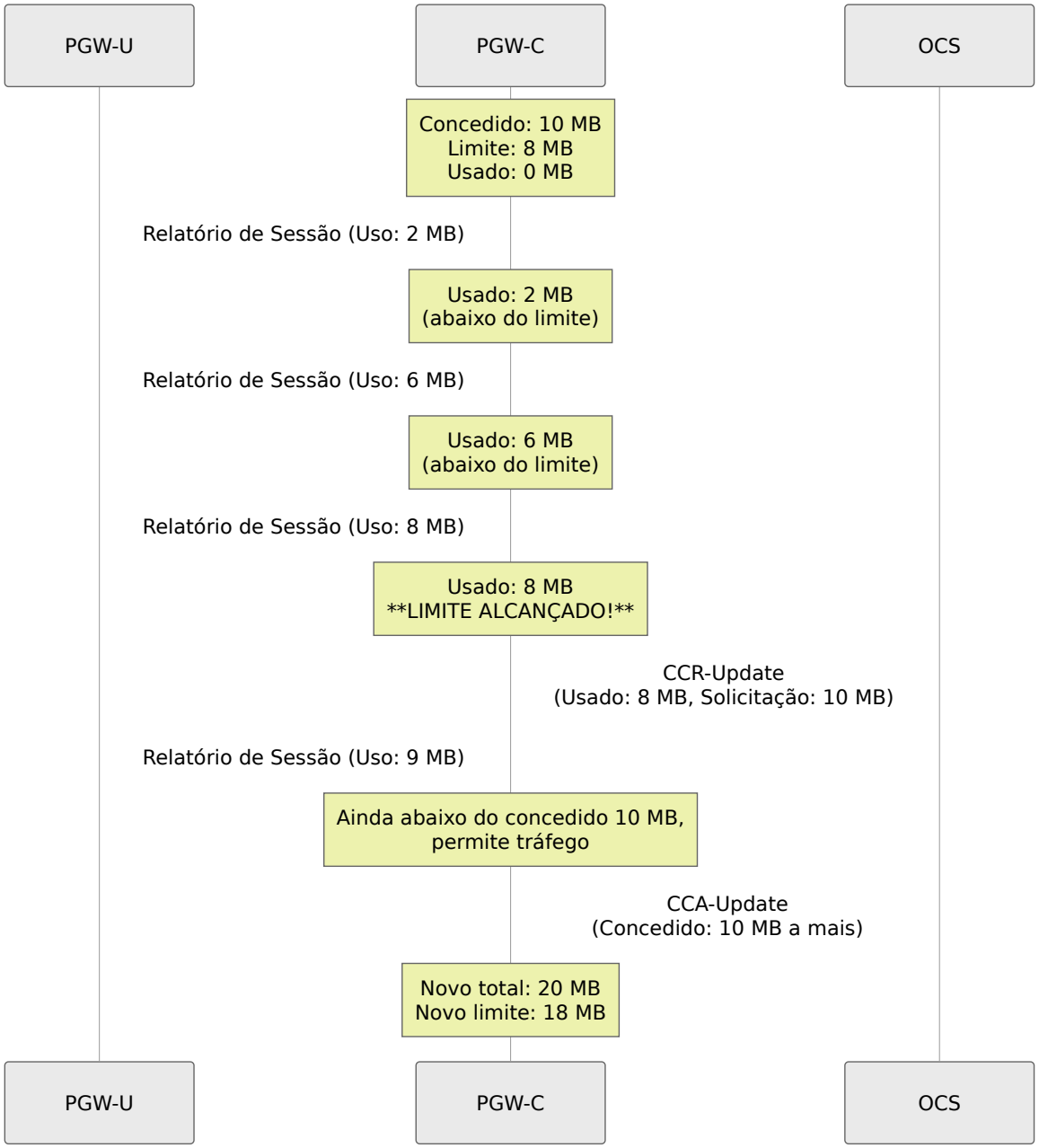
```
1. OCS concede cota de 10 MB com limite de 80% (8 MB)
2. PGW-C monitora o uso via relatórios de uso do PGW-U (Relatórios
de Sessão PFCP)
3. Quando o uso atinge 8 MB:
   → PGW-C envia CCR-Update
   → Continua permitindo tráfego (não espera pela resposta)
4. OCS responde com mais cota
5. Se a cota se esgotar antes do CCR-Update enviado:
   → PGW-C deve bloquear o tráfego
```

Cálculo do Limite:

```
Granted-Service-Unit: 10000000 bytes (10 MB)
Volume-Quota-Threshold: 8000000 bytes (8 MB)

Quando 8 MB consumidos → Acionar CCR-Update
Buffer restante: 2 MB (permite tempo para a resposta do OCS)
```

Monitoramento do PGW-C:

O PGW-C monitora o uso via **Relatórios de Sessão PFCP** do PGW-U:



Indicação da Unidade Final

O que acontece quando o crédito se esgota?

O OCS inclui o AVP **Final-Unit-Indication** no CCA para especificar a ação:

Ação da Unidade Final	Valor	Comportamento do PGW-C
TERMINATE	0	Bloquear todo o tráfego, iniciar o término da sessão
REDIRECT	1	Redirecionar tráfego para o portal (por exemplo, página de recarga)
RESTRICT_ACCESS	2	Permitir acesso apenas a serviços específicos (por exemplo, servidor de recarga)

Exemplo: Unidade Final com Redirecionamento

```
CCA (Atualização)
└── Multiple-Services-Credit-Control
    ├── Result-Code: DIAMETER_SUCCESS (2001)
    ├── Granted-Service-Unit
    │   └── CC-Total-Octets: 1000000 (último 1 MB)
    └── Final-Unit-Indication
        ├── Final-Unit-Action: REDIRECT (1)
        └── Redirect-Server (Grouped)
            ├── Redirect-Address-Type: URL (2)
            └── Redirect-Server-Address:
"http://topup.example.com"
```

Ações do PGW-C:

1. **TERMINATE:** Enviar CCR-T, excluir bearer
2. **REDIRECT:** Instalar regra PFCP para redirecionar HTTP para URL de recarga
3. **RESTRICT_ACCESS:** Instalar regras PFCP permitindo apenas IPs na lista branca

---

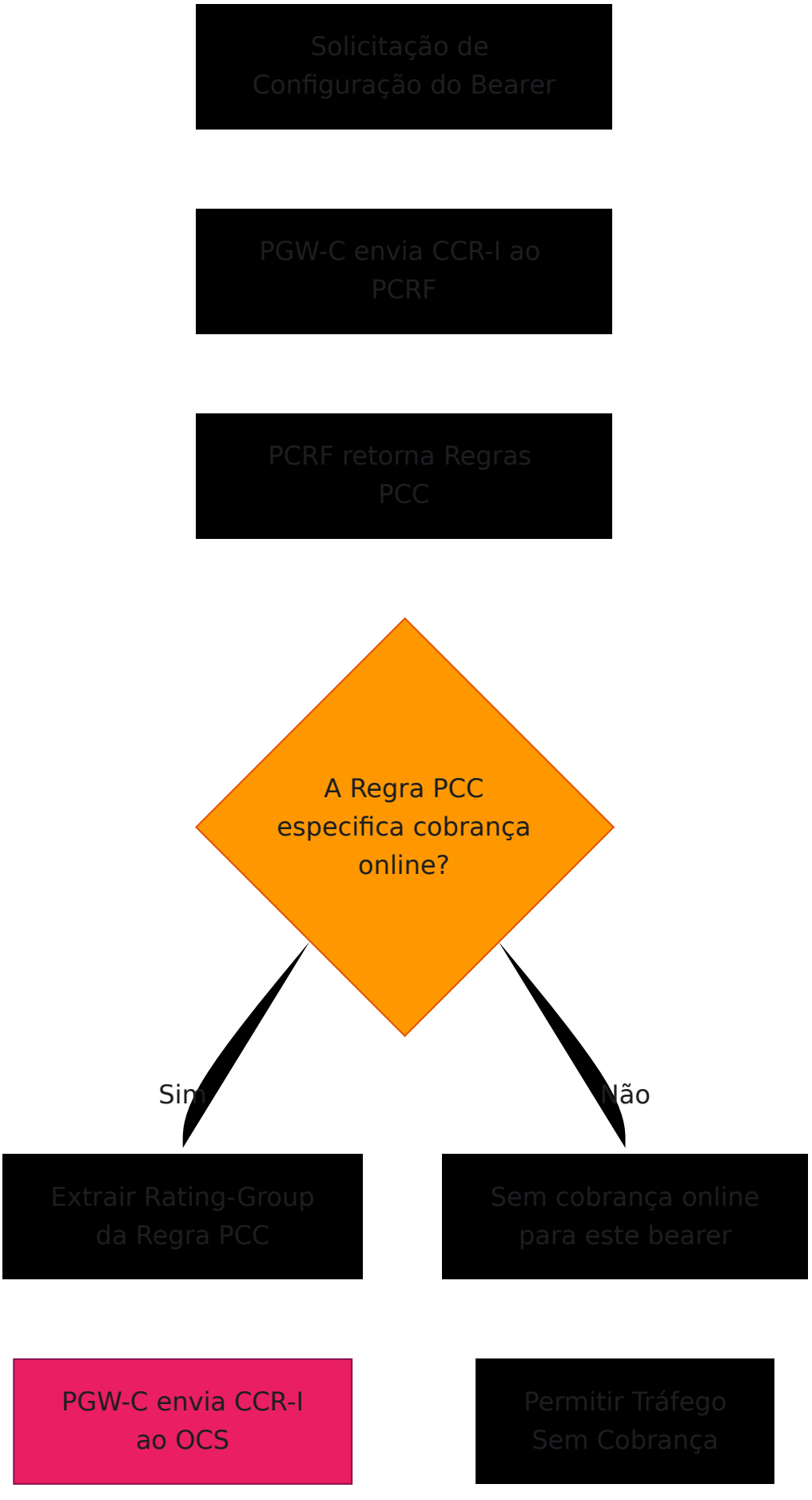
Controle de Cobrança de Bearer

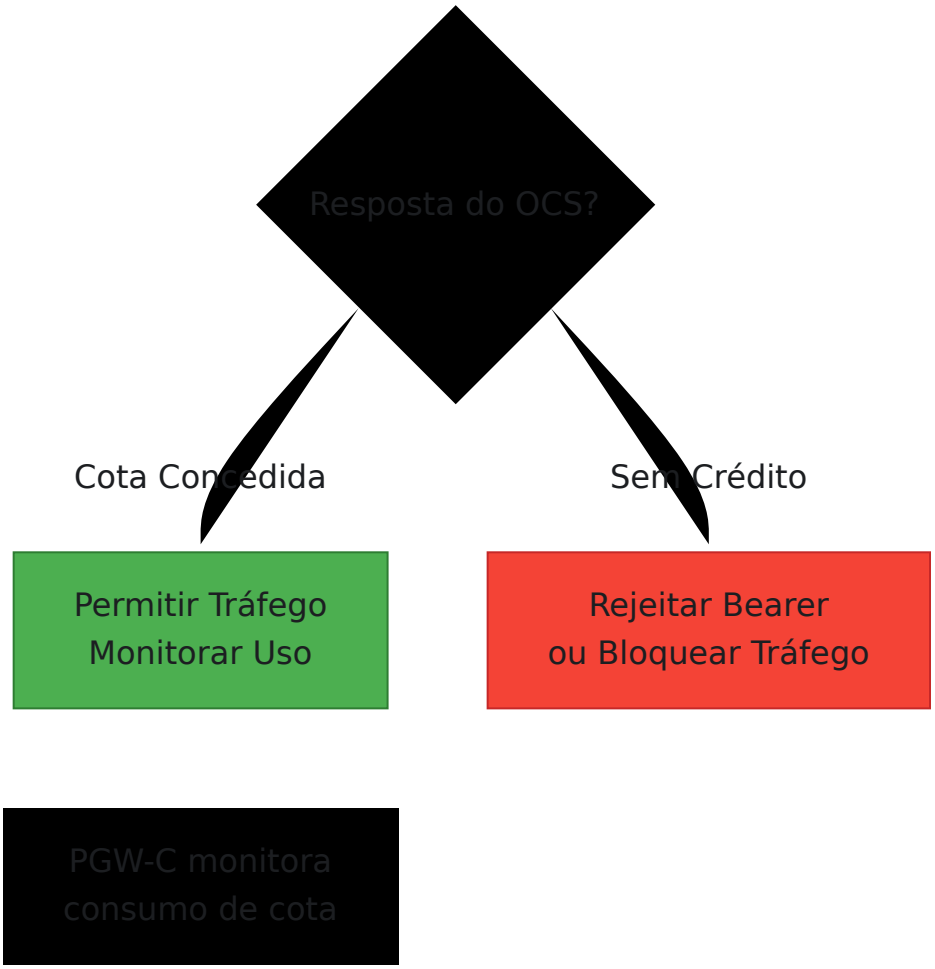
O que Controla se um Bearer é Cobrado?

Especificação 3GPP: TS 23.203, TS 29.212, TS 32.251

A cobrança do bearer é controlada por **Regras PCC** provisionadas pelo PCRF via a interface Gx. Veja Interface Diameter Gx para a documentação completa das regras PCC.

Fluxo de Decisão de Cobrança:


Solicitação de Configuração do Bearer
PGW-C envia CCR-I ao PCRF
PCRF retorna Regras PCC
A Regra PCC especifica cobrança online?
Sim
Não
Extrair Rating-Group da Regra PCC
Sem cobrança online para este bearer
PGW-C envia CCR-I ao OCS
Permitir Tráfego Sem Cobrança



Regra PCC com Informações de Cobrança

Resposta PCRF (CCA-I na Gx):

```
CCA (Interface Gx)
└── Charging-Rule-Definition (Grouped)
    ├── Charging-Rule-Name: "prepaid_data_rule"
    ├── Rating-Group: 100
    ├── Online: 1 (habilitar cobrança online)
    ├── Offline: 0 (desabilitar cobrança offline)
    ├── Metering-Method: VOLUME (1)
    ├── Precedence: 100
    ├── Flow-Information: [...]
    └── QoS-Information: [...]
```

Principais AVPs de Cobrança nas Regras PCC:

Nome do AVP	Código do AVP	Valores	Descrição
Rating-Group	432	Unsigned32	Categoria de cobrança (mapeia para tarifa no OCS)
Online	1009	0=Desabilitar, 1=Habilitar	Habilitar cobrança online (Gy)
Offline	1008	0=Desabilitar, 1=Habilitar	Habilitar cobrança offline (Gz)
Metering-Method	1007	0=Duração, 1=Volume, 2=Ambos	O que medir
Reporting-Level	1011	0=Serviço, 1=Grupo de Classificação	Granularidade dos relatórios de uso

Matriz de Decisão de Cobrança do Bearer

Online	Offline	Rating-Group	Comportamento
1	0	Presente	Cobrança online apenas (pré-pago)
0	1	Presente	Cobrança offline apenas (pós-pago)
1	1	Presente	Cobrança online e offline (convergente)
0	0	-	Sem cobrança (serviço gratuito)

Múltiplos Grupos de Classificação

Uma única conexão PDN pode ter **múltiplos bearers com diferentes grupos de classificação**:

Exemplo de Cenário:

```
Bearer Padrão (Internet)
├── Rating-Group: 100 (Dados Padrão)
└── Online: 1

Bearer Dedicado 1 (Streaming de Vídeo)
├── Rating-Group: 200 (Serviço de Vídeo)
└── Online: 1

Bearer Dedicado 2 (Voz IMS)
├── Rating-Group: 300 (Voz)
└── Online: 1
```

Comportamento do PGW-C Gy:

- **Único CCR-I** com múltiplas seções MSCC (Controle de Crédito para Múltiplos Serviços):

```
CCR-Initial
├── Session-Id: "..."
└── Multiple-Services-Credit-Control
    ├── [Rating-Group: 100] → Dados Padrão
    ├── [Rating-Group: 200] → Serviço de Vídeo
    └── [Rating-Group: 300] → Voz
```

Resposta do OCS:

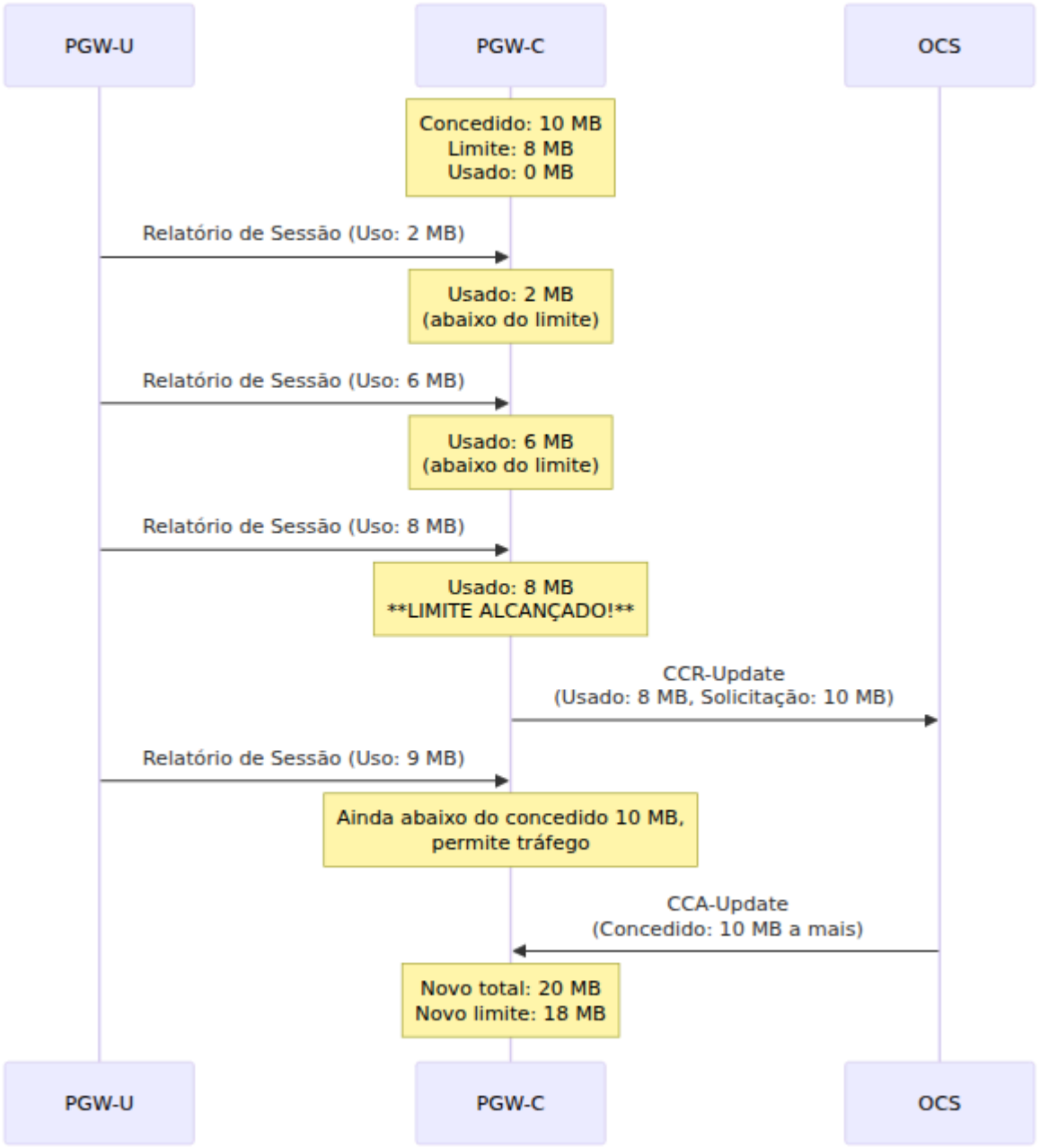
```
CCA-Initial
└── Multiple-Services-Credit-Control
    ├── [Rating-Group: 100] → Concedido: 10 MB
    ├── [Rating-Group: 200] → Concedido: 5 MB (vídeo mais caro)
    └── [Rating-Group: 300] → Concedido: 60 segundos
```

Aplicação de Cobrança por Serviço

O PGW-C rastreia a cota por Grupo de Classificação:

```
# Pseudocódigo
state.charging_quotas = %{
  100 => %{granted: 10_000_000, used: 0, threshold: 8_000_000},
  200 => %{granted: 5_000_000, used: 0, threshold: 4_000_000},
  300 => %{granted: 60_000, used: 0, threshold: 48_000}  #
milissegundos
}
```

Monitoramento de Uso por Bearer:



Controle de Crédito para Múltiplos Serviços

AVP MSCC (Controle de Crédito para Múltiplos Serviços)

Propósito: Agrupar informações de cobrança para um serviço/grupo de classificação específico

Estrutura:

```
Multiple-Services-Credit-Control (Grouped, AVP 456)
├── Service-Identifier (Unsigned32, AVP 439)
├── Rating-Group (Unsigned32, AVP 432)
├── Requested-Service-Unit (Grouped, AVP 437)
│   ├── CC-Time (Unsigned32, AVP 420)
│   ├── CC-Total-Octets (Unsigned64, AVP 421)
│   ├── CC-Input-Octets (Unsigned64, AVP 412)
│   └── CC-Output-Octets (Unsigned64, AVP 414)
├── Used-Service-Unit (Grouped, AVP 446)
│   └── [Mesma estrutura que Requested-Service-Unit]
├── Granted-Service-Unit (Grouped, AVP 431)
│   └── [Mesma estrutura que Requested-Service-Unit]
├── Validity-Time (Unsigned32, AVP 448)
├── Result-Code (Unsigned32, AVP 268)
└── Final-Unit-Indication (Grouped, AVP 430)
    └── Final-Unit-Action (Enumerated, AVP 449)
```

Service-Identifier vs. Rating-Group

Atributo	Service-Identifier	Rating-Group
Propósito	Identifica o tipo de serviço	Identifica a categoria de cobrança
Exemplo	1=Dados, 2=Voz, 3=SMS	100=Regular, 200=Premium
Granularidade	Classificação ampla	Tarifa específica
Requerido	Opcional	Requerido para cobrança
Mapeamento	Pode mapear para múltiplos RGs	Tarifa única no OCS

Exemplo:

```
Service-Identifier: 1 (Serviço de Dados)
├── Rating-Group: 100 (Dados Padrão - $0.01/MB)
└── Rating-Group: 200 (Dados Premium - $0.05/MB)

Service-Identifier: 2 (Voz)
└── Rating-Group: 300 (Chamadas de Voz - $0.10/min)
```

Configuração

Configuração Básica do Gy

Edite `config/runtime.exs`:

```
config :pgw_c,
  gy: %{
    # Habilitar ou desabilitar cobrança online globalmente
    enabled: true,

    # Tempo limite de conexão com o OCS (milissegundos)
    timeout_ms: 5000,

    # Solicitação de cota padrão (bytes) se não especificado pelo
PCRF
    default_requested_quota: 10_000_000,  # 10 MB

    # Porcentagem de limite para reautorização
    # (0.8 = acionar CCR-Update em 80% da cota consumida)
    quota_threshold_percentage: 0.8,

    # Ação quando ocorre timeout do OCS
    # Opções: :block, :allow
    timeout_action: :block,

    # Ação quando OCS retorna sem crédito
    # Opções: :terminate, :redirect
    no_credit_action: :terminate,

    # URL de redirecionamento para recarga (usada se
no_credit_action: :redirect)
    topup_redirect_url: "http://topup.example.com"
  },
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",

    # Configuração do peer OCS
    peer_list: [
      # PCRF para controle de política (Gx)
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.30",
        initiate_connection: true
      },
      # OCS para cobrança online (Gy)
```

```
      %{
        host: "ocs.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.40",
        initiate_connection: true
      }
    ]
  }
```

Parâmetros de Configuração Explicados

`enabled`

- `true`: Cobrança online ativa, mensagens CCR enviadas ao OCS
- `false`: Cobrança online desativada, sem mensagens Gy

`timeout_ms`

- Tempo a esperar pela resposta CCA do OCS
- Recomendado: 3000-5000 ms

`default_requested_quota`

- Cota padrão a solicitar se o PCRF não especificar
- Valores típicos: 1-100 MB

`quota_threshold_percentage`

- Acionar CCR-Update quando esta % da cota for consumida
- Recomendado: 0.75-0.85 (75%-85%)
- Maior = menos mensagens, mas risco de esgotamento de cota
- Menor = mais mensagens, mas mais seguro

`timeout_action`

- **`:block`** - Bloquear tráfego se o OCS não responder (mais seguro, previne perda de receita)
- **`:allow`** - Permitir tráfego se o OCS não responder (melhor UX, risco de receita)

`no_credit_action`

- `:terminate` - Excluir bearer quando o crédito se esgotar
- `:redirect` - Redirecionar para o portal de recarga

Configuração Específica para Ambiente

Produção (assinantes pré-pagos):

```
config :pgw_c,
  gy: %{
    enabled: true,
    timeout_action: :block,
    no_credit_action: :terminate,
    quota_threshold_percentage: 0.8
  }
```

Teste/Desenvolvimento:

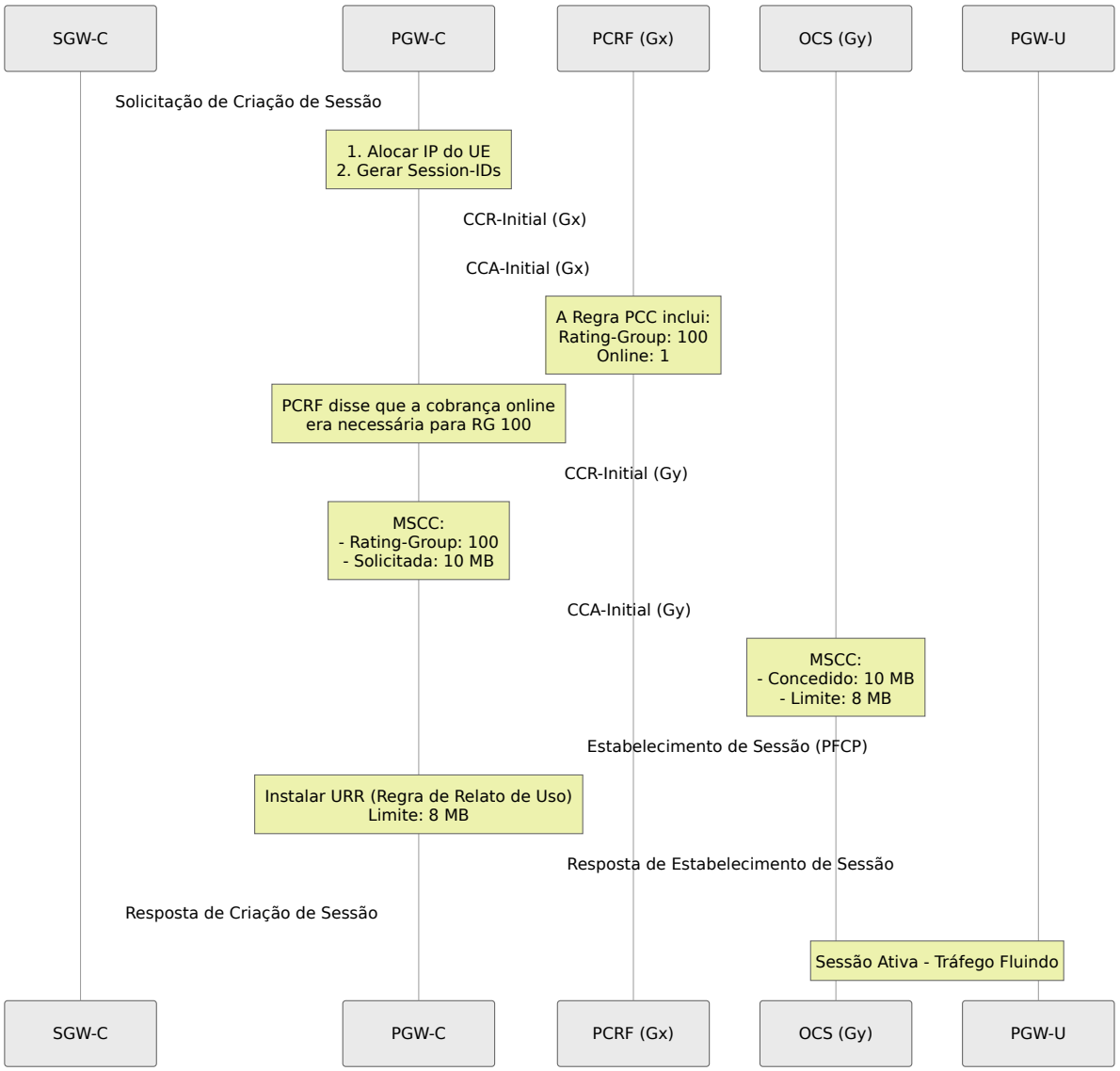
```
config :pgw_c,
  gy: %{
    enabled: false  # Desativar para testes
  }
```

Híbrido (alguns pré-pagos, alguns pós-pagos):

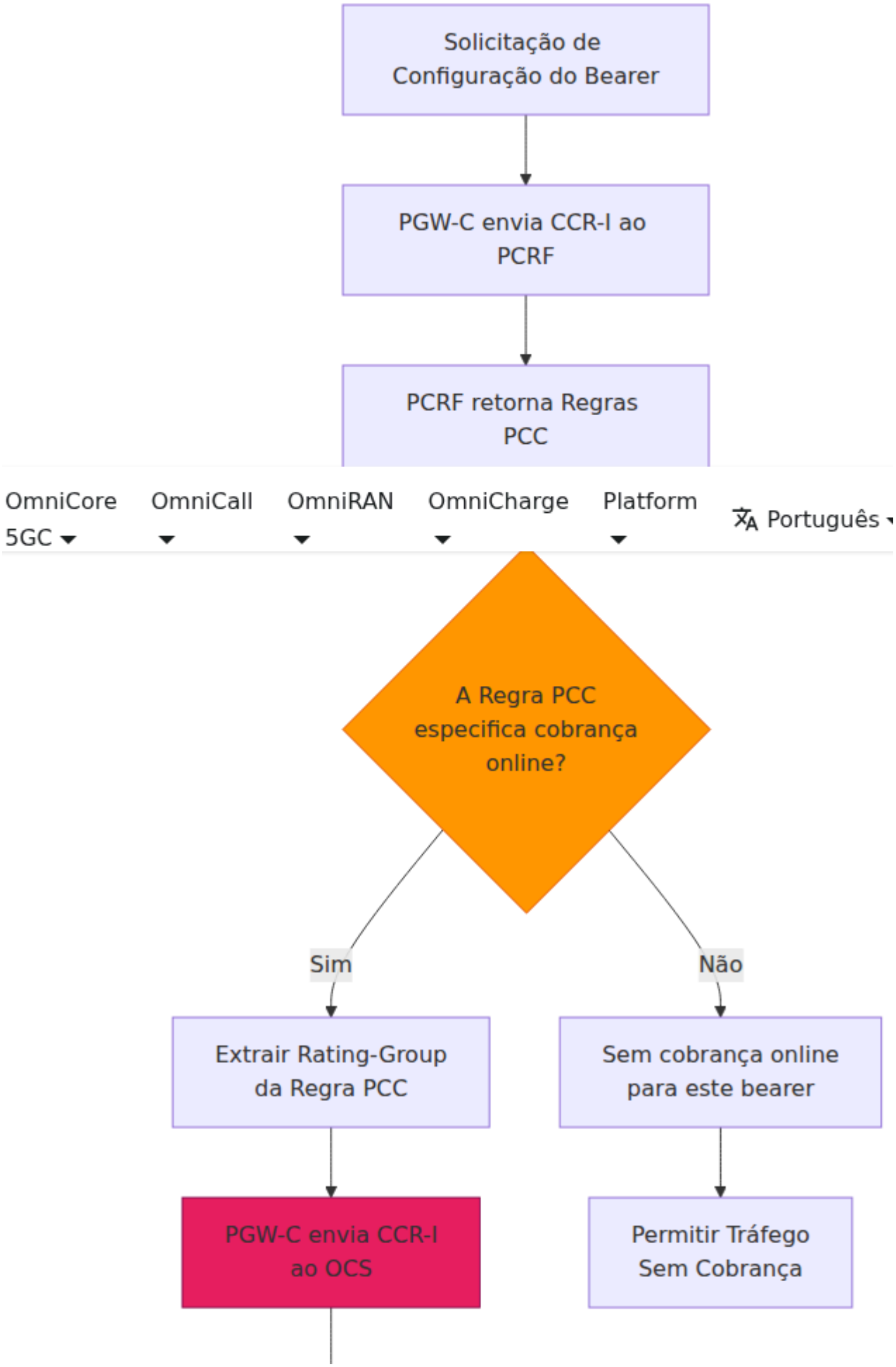
```
config :pgw_c,
  gy: %{
    enabled: true,  # Controlado por assinante pelo PCRF
    timeout_action: :allow,  # Não bloquear pós-pagos em falha do
OCS
    no_credit_action: :terminate
  }
```

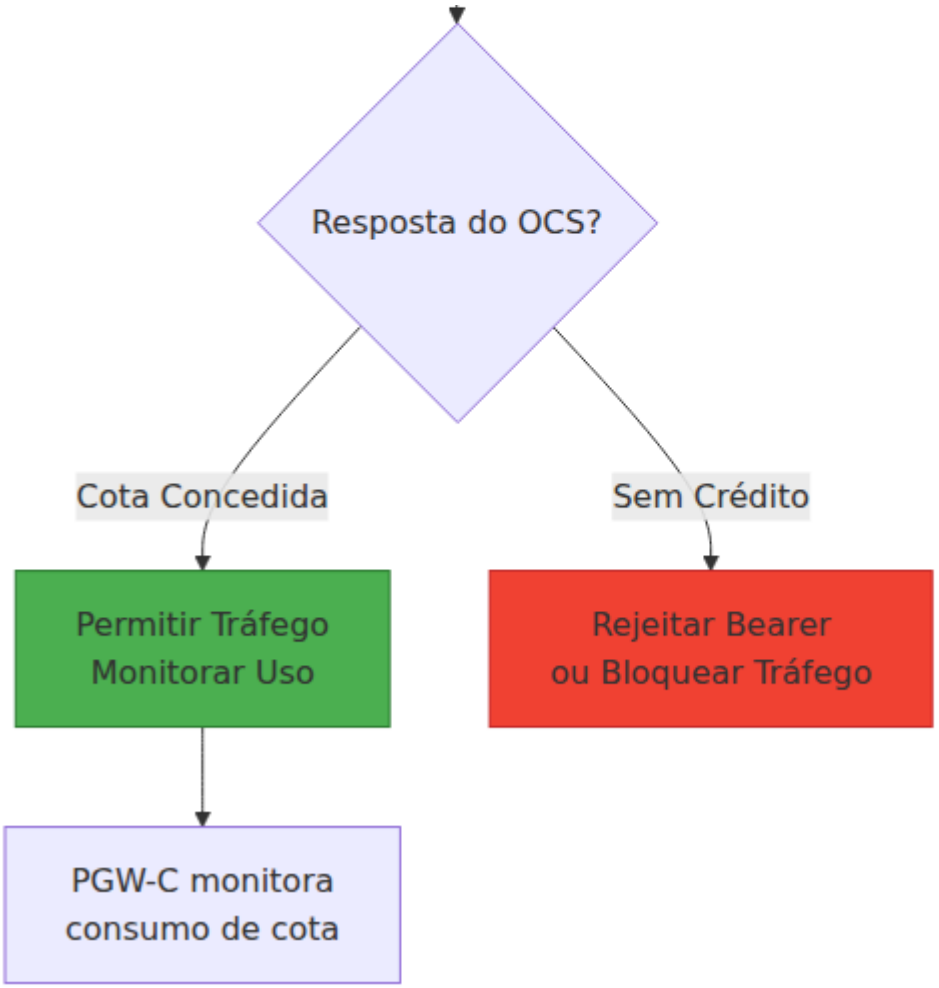
Fluxos de Mensagens

Sessão Bem-Sucedida com Cobrança Online

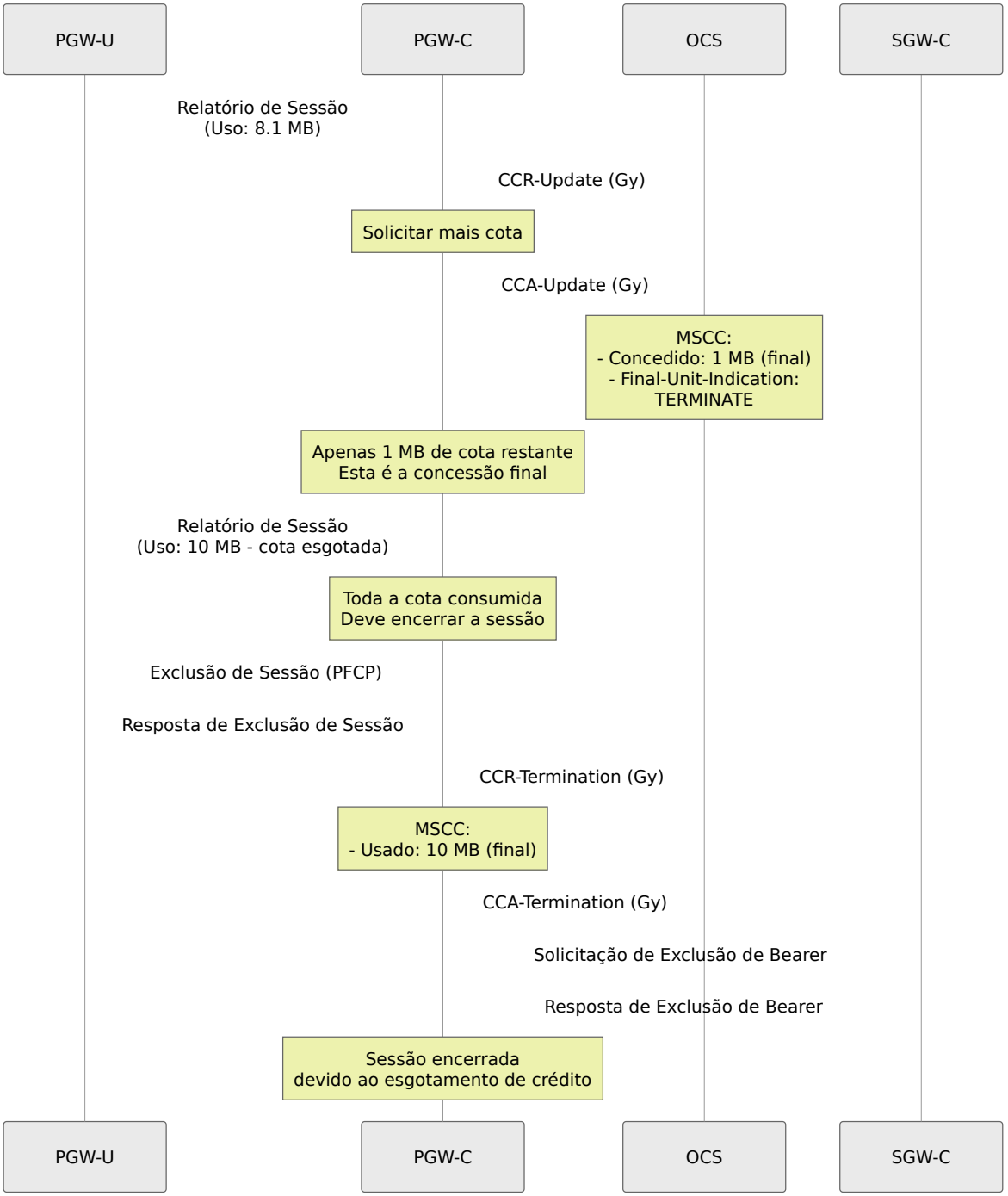


Reautorização de Cota (CCR-Update)

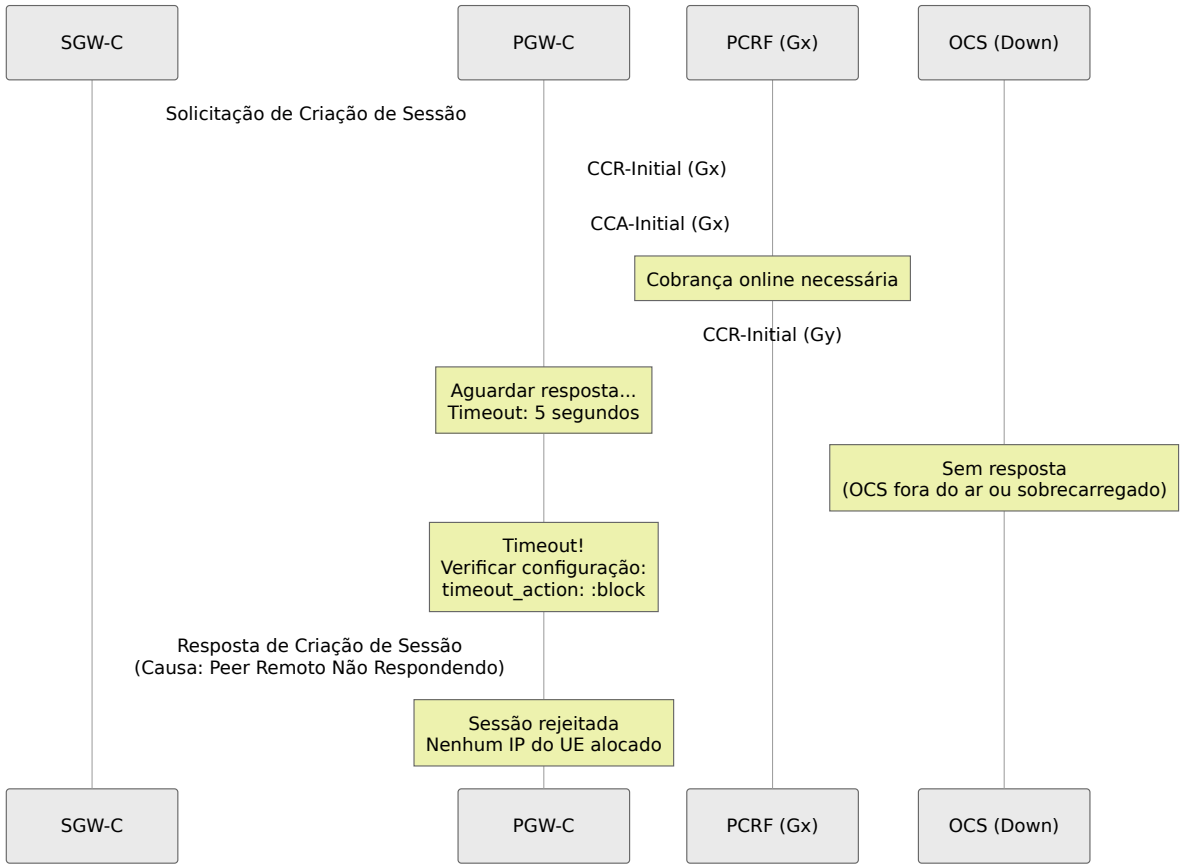

Solicitação de Configuração do Bearer
PGW-C envia CCR-I ao PCRF
PCRF retorna Regras PCC
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Português
A Regra PCC especifica cobrança online?
Sim
Não
Extrair Rating-Group da Regra PCC
Sem cobrança online para este bearer
PGW-C envia CCR-I ao OCS
Permitir Tráfego Sem Cobrança



Esgotamento de Crédito (Unidade Final)


PGW-U
PGW-C
OCS
SGW-C
Relatório de Sessão
(Uso: 8.1 MB)
CCR-Update (Gy)
Solicitar mais cota
CCA-Update (Gy)
MSCC:
- Concedido: 1 MB (final)
- Final-Unit-Indication:
TERMINATE
Apenas 1 MB de cota restante
Esta é a concessão final
Relatório de Sessão
(Uso: 10 MB - cota esgotada)
Toda a cota consumida
Deve encerrar a sessão
Exclusão de Sessão (PFCP)
Resposta de Exclusão de Sessão
CCR-Termination (Gy)
MSCC:
- Usado: 10 MB (final)
CCA-Termination (Gy)
Solicitação de Exclusão de Bearer
Resposta de Exclusão de Bearer
Sessão encerrada
devido ao esgotamento de crédito
PGW-U
PGW-C
OCS
SGW-C

Tratamento de Timeout do OCS



Tratamento de Erros

Códigos de Resultado

Códigos de Sucesso:

Código	Nome	Ação
2001	DIAMETER_SUCCESS	Continuar com a cota concedida

Falhas Transitórias (4xxx):

Código	Nome	Ação do PGW-C
4010	DIAMETER_TOO_BUSY	Tentar novamente com backoff
4011	DIAMETER_UNABLE_TO_COMPLY	Registrar erro, pode tentar novamente
4012	DIAMETER_CREDIT_LIMIT_REACHED	Encerrar ou redirecionar

Falhas Permanentes (5xxx):

Código	Nome	Ação do PGW-C
5003	DIAMETER_AUTHORIZATION_REJECTED	Rejeitar sessão
5031	DIAMETER_USER_UNKNOWN	Rejeitar sessão (assinante inválido)

Códigos de Resultado por Serviço

Importante: O Result-Code pode aparecer em **dois níveis**:

1. **Nível de mensagem** - Resultado geral
2. **Nível MSCC** - Resultado por serviço

Exemplo:

```
CCA-Initial
├── Result-Code: DIAMETER_SUCCESS (2001)  ← Nível de mensagem: OK
└── Multiple-Services-Credit-Control
    ├── [Rating-Group: 100]
    │   └── Result-Code: DIAMETER_SUCCESS (2001)  ← RG 100: OK
    └── [Rating-Group: 200]
        └── Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)  ←
RG 200: Sem crédito
```

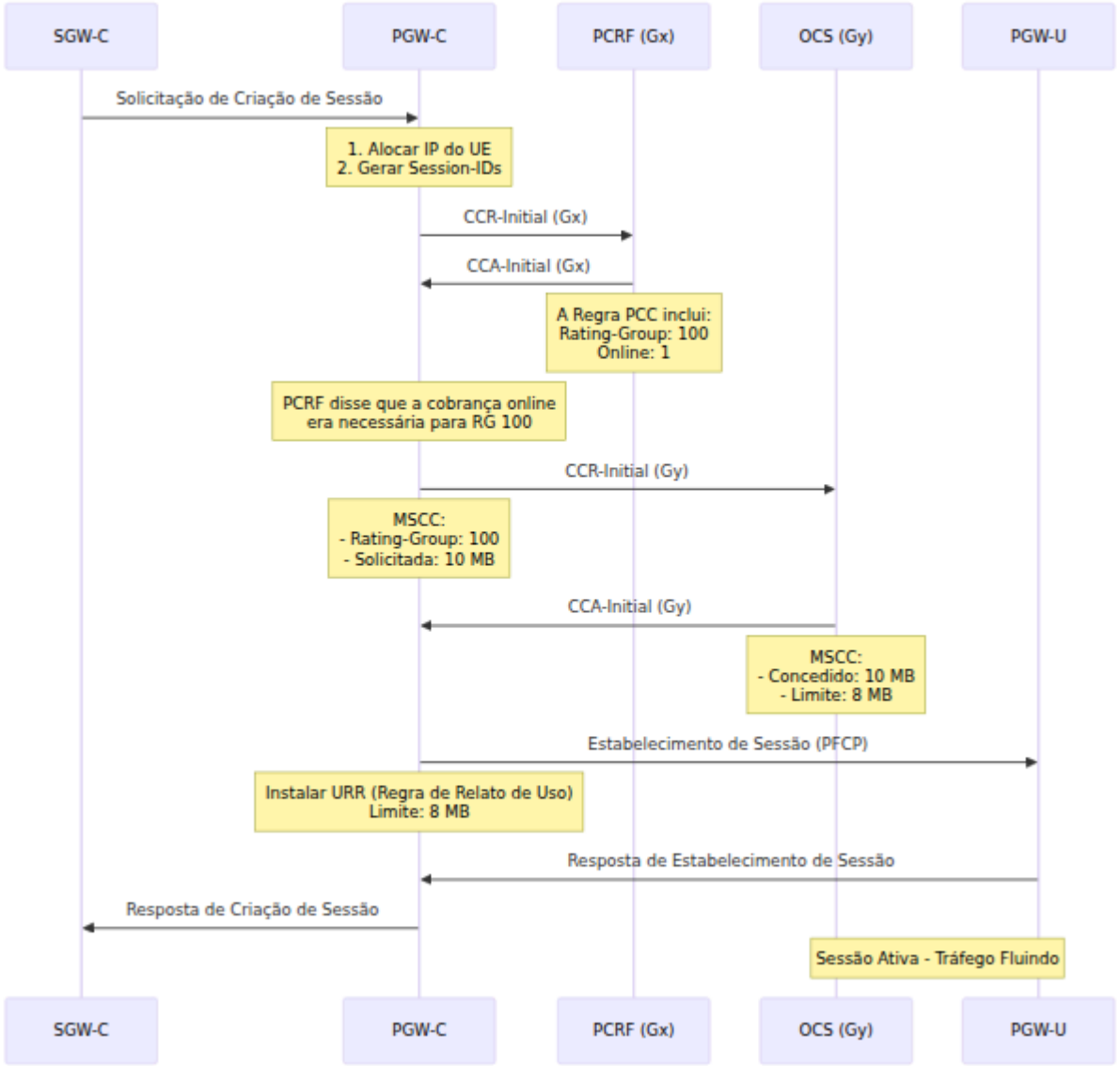
Comportamento do PGW-C:

- Permitir tráfego para o Rating-Group 100
- Bloquear tráfego para o Rating-Group 200

Integração com Gx

A interface Gx (controle de política PCRF) determina se a cobrança online é necessária e fornece o Rating-Group que impulsiona a cobrança Gy. Veja Interface Diameter Gx para a documentação completa de controle de política.

Relação entre Gx e Gy



Fluxo de Integração

1. Configuração do Bearer:

```
PGW-C recebe Solicitação de Criação de Sessão
    ↓
Enviar CCR-I ao PCRF (Gx)
    ↓
Receber CCA-I com Regras PCC
    ↓
Analisar Regras PCC:
    - A regra tem Rating-Group?
    - Está Online = 1?
    ↓
Se SIM:
    Enviar CCR-I ao OCS (Gy) com Rating-Group
    ↓
    Receber CCA-I com cota
    ↓
    Se cota concedida: Prosseguir
    Se sem crédito: Rejeitar bearer
Se NÃO:
    Prosseguir sem cobrança online
```

2. Atualização de Política Dinâmica (RAR do PCRF):

```
PCRF envia RAR (Re-Auth-Request) na Gx
    ↓
Nova Regra PCC adicionada com Online=1, Rating-Group=200
    ↓
PGW-C envia CCR-U ao OCS (Gy)
    - Adicionar MSCC para Rating-Group 200
    ↓
OCS concede cota para novo serviço
    ↓
Instalar bearer dedicado com cobrança online
```

Solução de Problemas

Problemas Comuns

1. Timeouts de CCR-Initial para OCS

Sintomas:

- Sessões falham com "timeout do OCS"
- Log: "timeout CCR-Initial (Gy)"

Possíveis Causas:

- OCS não acessível
- IP do OCS incorreto na configuração
- Firewall bloqueando a porta Diameter (3868)
- OCS sobrecarregado

Resolução:

```
# Testar conectividade de rede
ping <ocs_ip>

# Testar porta Diameter (TCP 3868)
telnet <ocs_ip> 3868

# Verificar configuração
# Garantir que o peer OCS esteja configurado na peer_list
```

2. Sessões Rejeitadas pelo OCS

Sintomas:

- CCA-I com Result-Code != 2001
- Falha na Resposta de Criação de Sessão

Códigos de Resultado Comuns:

Código de Resultado	Causa Provável	Resolução
4012	Limite de crédito alcançado	Assinante precisa recarregar
5003	Autorização rejeitada	Verificar permissões do assinante
5031	Usuário desconhecido	Provisionar assinante no OCS

Passos de Depuração:

1. Verificar logs do OCS para razão da rejeição
2. Verificar saldo do assinante no OCS
3. Verificar se IMSI/MSISDN no CCR-I corresponde ao registro do assinante

3. Esgotamento de Cota Não Detectado

Sintomas:

- Usuário continua usando dados após saldo esgotado
- Nenhum CCR-Update enviado

Possíveis Causas:

- URR (Regra de Relato de Uso) não instalada no PGW-U
- Limite não configurado corretamente
- Relatórios de Sessão PFCP não recebidos

Passos de Depuração:

1. Verificar URR na Estabelecimento de Sessão PFCP:

```
Criar URR
├── URR-ID: 1
├── Measurement-Method: VOLUME
├── Volume-Threshold: 8000000 (8 MB)
└── Reporting-Triggers: VOLUME_THRESHOLD
```

2. Verificar logs do PGW-U para relatórios de uso
3. Verificar `quota_threshold_percentage` na configuração

4. Grupo de Classificação Incorreto

Sintomas:

- OCS rejeita com "Grupo de Classificação Desconhecido"
- Sessões falham

Causa:

- Grupo de Classificação no CCR-I não corresponde à configuração do OCS
- PCRF provisionou Grupo de Classificação inválido

Resolução:

1. Verificar Grupo de Classificação na Regra PCC do PCRF
2. Verificar configuração do OCS para Grupos de Classificação válidos
3. Garantir mapeamento entre Regras PCC e tarifas do OCS

Monitoramento

Métricas Chave

```
# Taxas de mensagens Gy
rate(gy_inbound_messages_total{message_type="cca"}[5m])
rate(gy_outbound_messages_total{message_type="ccr"}[5m])

# Taxas de erro Gy
rate(gy_inbound_errors_total[5m])

# Eventos de esgotamento de cota
rate(gy_quota_exhausted_total[5m])

# Taxa de timeout do OCS
rate(gy_timeout_total[5m])

# Duração do manuseio de mensagens Gy
histogram_quantile(0.95,
rate(gy_inbound_handling_duration_bucket[5m]))
```

Alertas

```
# Alerta sobre alta taxa de erro Gy
- alert: GyErrorRateHigh
  expr: rate(gy_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Alta taxa de erro Gy detectada"

# Alerta sobre timeout do OCS
- alert: OcsTimeout
  expr: rate(gy_timeout_total[5m]) > 0.05
  for: 2m
  annotations:
    summary: "Timeouts do OCS ocorrendo"

# Alerta sobre pico de esgotamento de crédito
- alert: CreditExhaustionSpike
  expr: rate(gy_quota_exhausted_total[5m]) > 10
  for: 5m
  annotations:
    summary: "Alta taxa de esgotamento de crédito"
```

Interface Web - Simulador de Controle de Crédito Gy

OmniPGW inclui um simulador Gy/Ro embutido para testar a funcionalidade de cobrança online sem exigir um OCS externo.

Acesso: `http://<omnipgw-ip>:<web-port>/gy_simulator`

Propósito: Testar e simular cenários de cobrança online para assinantes pré-pagos

Recursos:

1. Parâmetros de Solicitação

- **IMSI** - Identidade do assinante (por exemplo, "310170123456789")
- **MSISDN** - Número de telefone (por exemplo, "14155551234")
- **Unidades Solicitadas** - Quantidade de cota a solicitar (em bytes)
- **ID do Serviço** - Identificador do tipo de serviço
- **Grupo de Classificação** - Categoria de cobrança

2. Simulação CCR-I

- Enviar CCR-Initial (Solicitação de Controle de Crédito Inicial)
- Simula solicitação de cota inicial durante o estabelecimento da sessão
- Testa a integração com o OCS sem tráfego ao vivo

3. Casos de Uso

- **Teste de Desenvolvimento** - Testar interface Gy durante o desenvolvimento

- **Integração com OCS** - Verificar conectividade e respostas do OCS
- **Teste de Cota** - Testar diferentes cenários de cota
- **Solução de Problemas** - Depurar problemas de cobrança
- **Demonstração** - Demonstrar cobrança online para partes interessadas

Como Usar:

```
1. Insira os detalhes do assinante (IMSI, MSISDN)
2. Defina as unidades solicitadas (por exemplo, 1000000 para 1 MB)
3. Configure ID do Serviço e Grupo de Classificação
4. Clique em "Enviar CCR-I"
5. Visualize a resposta do OCS e a cota concedida
```

Benefícios:

- Sem necessidade de OCS externo durante os testes
- Validação rápida da lógica de cobrança
- Ambiente de teste seguro
- Útil para treinamento e demonstrações

Documentação Relacionada

Cobrança e Política

- **Interface Diameter Gx** - Controle de política PCRF, regras PCC que acionam cobrança online
- **Formato CDR de Dados** - Registros de cobrança offline para faturamento pós-pago
- **Guia de Configuração** - Parâmetros completos de configuração de cobrança online

Gerenciamento de Sessão

- **Gerenciamento de Sessão** - Ciclo de vida da sessão PDN, gerenciamento de bearer
- **Interface PFCP** - Relato de uso do PGW-U via URRs
- **Interface S5/S8** - Configuração e desmontagem do bearer GTP-C

Operações

- **Guia de Monitoramento** - Métricas Gy, rastreamento de cota, alertas de timeout do OCS
- **Alocação de IP do UE** - Configuração do pool de IP para sessões cobradas

---

Voltar ao Guia de Operações

Documentação da Interface Gn/Gp

Comunicação GTP-C com SGSN (Redes 2G/3G)

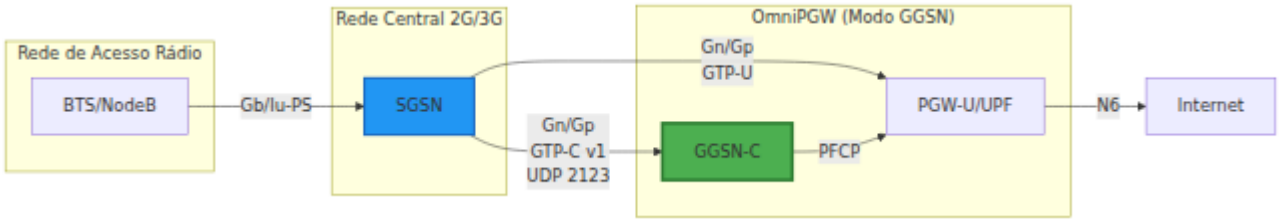
OmniPGW da Omnitouch Network Services

Visão Geral

A **interface Gn/Gp** permite que o OmniPGW funcione como um **GGSN** (Gateway GPRS Support Node) para redes 2G/3G usando o protocolo **GTP-C v1**. Esta interface gerencia o contexto PDP (Packet Data Protocol) entre o GGSN e os SGSNs.

- **Interface Gn**: Conecta-se aos SGSNs dentro do mesmo PLMN (rede doméstica)
- **Interface Gp**: Conecta-se aos SGSNs em outros PLMNs (cenários de roaming)

Ambas as interfaces usam protocolos idênticos - a distinção é puramente topológica.



Diferenças Chave em Relação ao PGW (S5/S8)

Aspecto	GGSN (Gn/Gp)	PGW (S5/S8)
Versão do Protocolo	GTP-C v1	GTP-C v2
Especificação 3GPP	TS 29.060	TS 29.274
Conceito de Sessão	Contexto PDP	Sessão PDN + Portadoras
Identificador de Portadora	NSAPI (0-15)	EBI (5-15)
Interface de Política	Nenhuma (política estática)	Gx (PCRF)
Modelo QoS	Perfil QoS R99	QoS de Portadora EPS (QCI)
Porta	2123 (compartilhada)	2123

Detalhes do Protocolo

GTP-C Versão 1

- **Protocolo**: GTP-C v1 (3GPP TS 29.060)
- **Transporte**: UDP
- **Porta**: 2123 (compartilhada com S5/S8 GTP-C v2)
- **Tipo de Interface**: Plano de Controle

TEID (Identificador de Ponto de Extremidade do Túnel)

Cada contexto PDP possui TEIDs únicos para controle e plano de usuário:

- **TEID de Controle do GGSN**: Alocado pelo OmniPGW para mensagens de controle recebidas
- **TEID de Dados do GGSN**: Alocado pelo UPF para dados de usuário recebidos
- **TEID de Controle do SGSN**: Fornecido pelo SGSN para mensagens de controle enviadas
- **TEID de Dados do SGSN**: Fornecido pelo SGSN para dados de usuário enviados

```
Fluxo da Mensagem:
  SGSN → GGSN: TEID de Destino = TEID de Controle do GGSN
  GGSN → SGSN: TEID de Destino = TEID de Controle do SGSN
```

Suporte a CUPS (Separação de Controle e Plano de Usuário)

O OmniPGW suporta a arquitetura CUPS para 2G/3G:

- **Endereço GSN para Sinalização**: IP do plano de controle do OmniPGW (de `gn.local_ipv4_address`)
- **Endereço GSN para Tráfego de Usuário**: Endereço IP do UPF (da Resposta de Estabelecimento de Sessão PFCP)

Isso permite que o GGSN-C e o PGW-U/UPF operem em nós separados com endereços IP diferentes, o que é padrão para implantações CUPS.

NSAPI (Identificador de Ponto de Acesso ao Serviço de Rede)

O NSAPI identifica contextos PDP individuais dentro de uma sessão de assinante:

- **Faixa**: 5-15 (0-4 reservados)
- **Uso**: Múltiplos contextos PDP por assinante são possíveis
- **Equivalente**: Semelhante ao EBI em LTE/EPC

Configuração

Configuração Básica

```
# config/runtime.exs
config :pgw_c,
  # A interface Gn/Gp é habilitada automaticamente quando a
configuração gn está presente
  gn: %{
    # Endereço IPv4 local para a interface Gn
    local_ipv4_address: "10.0.0.20",

    # Opcional: Endereço IPv6 local
    local_ipv6_address: nil,

    # Porta para GTP-C v1 (compartilhada com S5/S8)
    local_port: 2123
  },

  # Servidores DNS retornados em PCO (compartilhados com PGW)
  dns: %{
    primary_ipv4: {8, 8, 8, 8},
    secondary_ipv4: {8, 8, 4, 4}
  }
```

Parâmetros da Interface Gn

Parâmetro	Tipo	Requerido	Padrão	Descrição
`local_ipv4_address`	String	Sim	-	Endereço IPv4 para vincular à interface Gn. Este é o endereço do GGSN anunciado aos SGSNs.
`local_ipv6_address`	String	Não	`nil`	Endereço IPv6 opcional. A maioria das redes 2G/3G é apenas IPv4.
`local_port`	Integer	Não	2123	Porta UDP para GTP-C. Porta padrão conforme 3GPP TS 29.060. Compartilhada com S5/S8.

Parâmetros DNS

Parâmetro	Tipo	Requerido	Padrão	Descrição
`primary_ipv4`	Tuple	Não	`{8, 8, 8, 8}`	Endereço IPv4 do servidor DNS primário retornado em PCO.
`secondary_ipv4`	Tuple	Não	`{8, 8, 4, 4}`	Endereço IPv4 do servidor DNS secundário retornado em PCO.
`primary_ipv6`	Tuple	Não	`nil`	Endereço IPv6 do servidor DNS primário.
`secondary_ipv6`	Tuple	Não	`nil`	Endereço IPv6 do servidor DNS secundário.

Requisitos de Rede

Regras de Firewall:

```
# Permitir GTP-C da rede SGSN
iptables -A INPUT -p udp --dport 2123 -s <sgsn_network>/24 -j
ACCEPT

# Permitir GTP-C de saída para SGSN
iptables -A OUTPUT -p udp --dport 2123 -d <sgsn_network>/24 -j
ACCEPT
```

Tipos de Mensagens

Gerenciamento de Contexto PDP

Solicitação de Criação de Contexto PDP

Direção: SGSN → GGSN

Propósito: Estabelecer um novo contexto PDP para conectividade de dados

Principais IEs (Elementos de Informação):

Nome do IE	Tipo	Descrição
IMSI	Identidade	Identidade Internacional do Assinante Móvel
NSAPI	Inteiro	Identificador de Ponto de Acesso ao Serviço de Rede (5-15)
TEID Dados I	Inteiro	Ponto de extremidade do túnel do plano de usuário do SGSN
TEID Controle	Inteiro	Ponto de extremidade do túnel do plano de controle do SGSN
Endereço do Usuário Final	Endereço	Tipo de PDN solicitado e IP opcional
Nome do Ponto de Acesso	String	APN para a conexão
Endereço GSN (Sinalização)	IP	Endereço do plano de sinalização do SGSN
Endereço GSN (Usuário)	IP	Endereço do plano de usuário do SGSN
Perfil QoS	Binário	Parâmetros QoS solicitados
MSISDN	Identidade	Número de telefone móvel (opcional)
Modo de Seleção	Enum	Modo de seleção de APN
Opções de Configuração de Protocolo	Opções	Opções de protocolo adicionais

Exemplo:

```
Solicitação de Criação de Contexto PDP
├── IMSI: 310260123456789
├── NSAPI: 5
├── TEID Dados I: 0x12345678
├── TEID Controle: 0x87654321
├── Endereço do Usuário Final: IPv4 (dinâmico)
├── APN: internet
├── Endereço GSN (Sinalização): 10.1.1.100
├── Endereço GSN (Usuário): 10.1.1.100
├── Perfil QoS: [Parâmetros QoS R99]
└── PCO: [Solicitação DNS, etc.]
```

Resposta de Criação de Contexto PDP

Direção: GGSN → SGSN

Propósito: Reconhecer a criação do contexto PDP com recursos alocados

Principais IEs:

Nome do IE	Tipo	Descrição
Causa	Resultado	Código de sucesso ou erro
Reordenação Necessária	Booleano	Se a reordenação é necessária
Recuperação	Contador	Contador de reinicialização do GGSN
TEID Dados I	Inteiro	Ponto de extremidade do túnel do plano de usuário do GGSN
TEID Controle	Inteiro	Ponto de extremidade do túnel do plano de controle do GGSN
NSAPI	Inteiro	NSAPI confirmado
ID de Cobrança	Binário	ID de correlação de cobrança
Endereço do Usuário Final	Endereço	Endereço IP do UE alocado
Endereço GSN (Sinalização)	IP	Endereço do plano de sinalização do GGSN
Endereço GSN (Usuário)	IP	Endereço do plano de usuário do GGSN
Perfil QoS	Binário	Parâmetros QoS negociados
Opções de Configuração de Protocolo	Opções	Servidores DNS, etc.

Resposta de Sucesso:

```
Resposta de Criação de Contexto PDP
├── Causa: Solicitação Aceita (128)
├── TEID Dados I: 0xAABBCCDD
├── TEID Controle: 0xDDCCBBAA
├── NSAPI: 5
├── ID de Cobrança: 0x11223344
├── Endereço do Usuário Final
│   └── IPv4: 100.64.1.42
├── Endereço GSN (Sinalização): 10.0.0.20
├── Endereço GSN (Usuário): 10.0.0.20
├── Perfil QoS: [QoS Negociado]
└── PCO
    ├── DNS Primário: 8.8.8.8
    └── DNS Secundário: 8.8.4.4
```

Solicitação de Atualização de Contexto PDP

Direção: SGSN → GGSN

Propósito: Modificar um contexto PDP existente (por exemplo, realocação do SGSN, alteração de QoS)

Cenários comuns:

- Handover Inter-SGSN (atualização da área de roteamento)
- Renegociação de QoS
- Mudança de endereço do SGSN

Principais IEs:

Nome do IE	Descrição
NSAPI	Identificador do contexto PDP
TEID Dados I	Novo TEID do plano de usuário do SGSN
Endereço GSN	Novos endereços do SGSN
Perfil QoS	QoS atualizada (opcional)

Resposta de Atualização de Contexto PDP

Direção: GGSN → SGSN

Propósito: Reconhecer a atualização do contexto PDP

Principais IEs:

Nome do IE	Descrição
Causa	Código de sucesso ou erro
TEID Dados I	TEID do plano de usuário do GGSN
Endereço GSN	Endereços do GGSN
Perfil QoS	QoS negociada

Solicitação de Exclusão de Contexto PDP

Direção: SGSN → GGSN

Propósito: Terminar um contexto PDP

Principais IEs:

Nome do IE	Descrição
NSAPI	Contexto PDP a ser excluído
Indicação de Desmontagem	Excluir todos os contextos para este assinante

Resposta de Exclusão de Contexto PDP

Direção: GGSN → SGSN

Propósito: Reconhecer a exclusão do contexto PDP

Principais IEs:

Nome do IE	Descrição
Causa	Código de sucesso ou erro

Gerenciamento de Caminhos

Solicitação / Resposta de Eco

Direção: Bidirecional

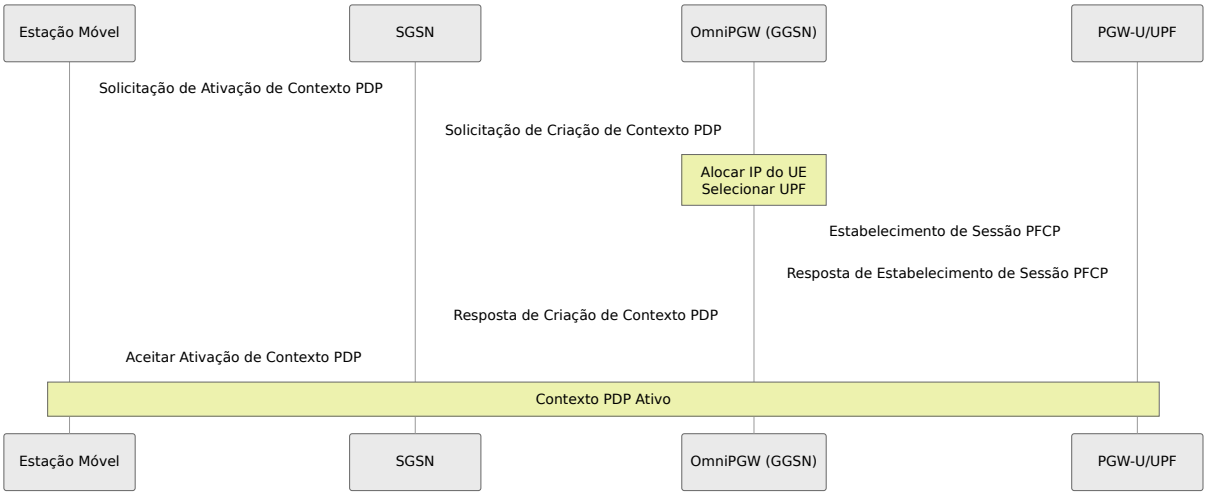
Propósito: Manter o caminho ativo e detectar reinicializações

Principais IEs:

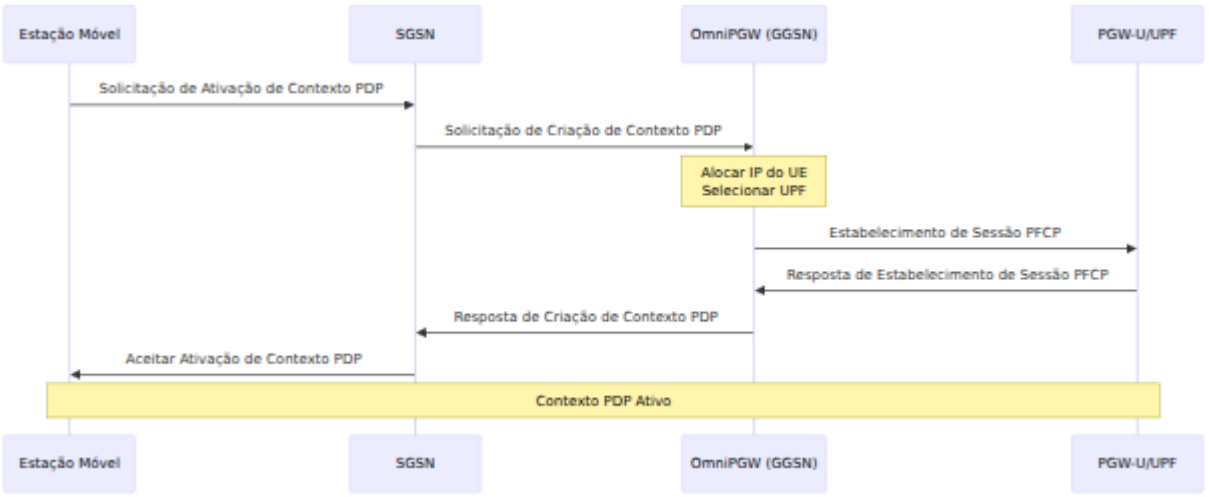
Nome do IE	Descrição
Recuperação	Contador de reinicialização para detectar reinicializações de nó

Fluxos de Mensagem

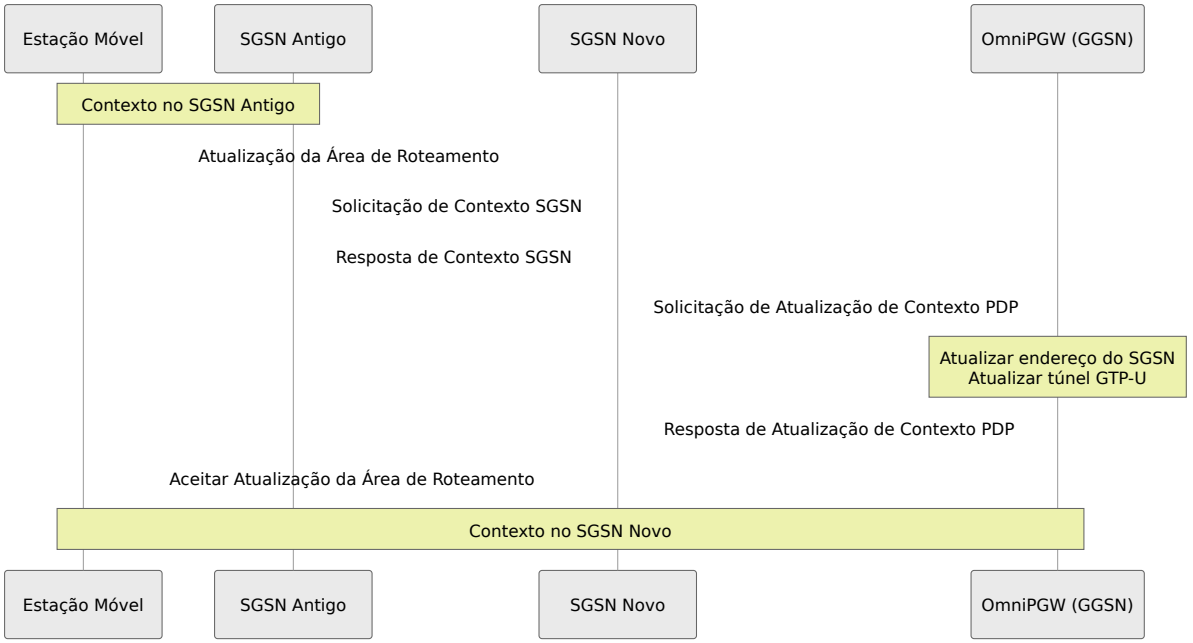
Ativação do Contexto PDP



Desativação do Contexto PDP



Handover Inter-SGSN



Infraestrutura Compartilhada

A funcionalidade GGSN do OmniPGW compartilha infraestrutura com o modo PGW:

Alocação de Endereço IP do UE

Usa o mesmo AddressRegistry e configuração de sub-rede que o PGW. Veja Alocação de IP do UE para detalhes de configuração.

Gerenciamento de Sessão UPF/PFCP

Usa o mesmo estabelecimento de sessão PFCP que o PGW:

- Regras PDR/FAR/QER criadas por contexto PDP
- Seleção de UPF via a mesma configuração upf_selection
- Veja Interface PFCP para detalhes

Cobrança Online (Gy)

Integração opcional com Diameter Gy disponível:

- Controle de crédito para assinantes pré-pagos
- Mesma configuração Gy que o modo PGW
- Veja Interface Diameter Gy para configuração

Geração de CDR

Usa a mesma geração de CDR que o PGW. Veja Formato de CDR de Dados para detalhes.

Códigos de Causa

Sucesso

Código	Nome	Descrição
128	Solicitação Aceita	Operação bem-sucedida

Causas de Rejeição

Código	Nome	Quando Usado
192	Não existente	Contexto PDP não encontrado
193	Formato de mensagem inválido	Mensagem GTP malformada
194	IMSI desconhecido	Assinante não encontrado
195	MS está Desconectado do GPRS	MS não anexado
196	MS não está Respondendo ao GPRS	MS inacessível
197	MS Recusa	MS rejeitou a solicitação
198	Versão não suportada	Incompatibilidade de versão GTP
199	Nenhum recurso disponível	Exaustão de recursos
200	Serviço não suportado	Serviço não suportado
201	IE obrigatório incorreto	Validação de IE falhou
202	IE obrigatório ausente	IE necessário ausente
203	IE opcional incorreto	IE opcional inválido
204	Falha do sistema	Erro interno
205	Restrição de roaming	Roaming não permitido
206	Desvio de Assinatura P-TMSI	Falha de segurança
207	Conexão GPRS suspensa	Conexão suspensa

Código	Nome	Quando Usado
208	Falha de autenticação	Autenticação falhou
209	Falha na autenticação do usuário	Autenticação do usuário falhou

---

Monitoramento

Métricas da Interface Gn

```
# Contadores de mensagens
gn_inbound_messages_total{message_type="create_pdp_context_request"}
gn_inbound_messages_total{message_type="update_pdp_context_request"}
gn_inbound_messages_total{message_type="delete_pdp_context_request"}

gn_outbound_messages_total{message_type="create_pdp_context_response"
gn_outbound_messages_total{message_type="update_pdp_context_response"
gn_outbound_messages_total{message_type="delete_pdp_context_response"

# Latência de transação
gn_outbound_transaction_duration_bucket
```

Consultas Úteis

Taxa de Criação de PDP Contexto:

```
rate(gn_inbound_messages_total{message_type="create_pdp_context_reque
[5m])
```

Taxa de Sucesso:

```
sum(rate(gn_outbound_messages_total{message_type="create_pdp_context_
[5m]))
  /
sum(rate(gn_inbound_messages_total{message_type="create_pdp_context_r
[5m]))
```

Contextos PDP Ativos:

```
gn_inbound_messages_total{message_type="create_pdp_context_request"}
  -
gn_inbound_messages_total{message_type="delete_pdp_context_request"}
```

Solução de Problemas

Problema: Sem Resposta à Solicitação de Criação de PDP Contexto

Sintomas:

- SGSN envia Solicitação de Criação de PDP Contexto
- Nenhuma resposta recebida
- Timeout no SGSN

Causas possíveis:

1. Problema de conectividade de rede
2. OmniPGW não ouvindo no IP configurado
3. Firewall bloqueando UDP 2123
4. Falha no estabelecimento de UPF/PFCP

Depuração:

```
# Verifique se o OmniPGW está ouvindo
netstat -ulnp | grep 2123

# Verifique pacotes recebidos
tcpdump -i any -n port 2123

# Verifique a configuração
grep "local_ipv4_address" config/runtime.exs

# Verifique a conectividade PFCP
curl http://pgw:9090/metrics | grep pfcp
```

Problema: Criação de Contexto PDP Rejeitada

Sintomas:

- Resposta de Criação de PDP Contexto com causa de erro
- Contexto PDP não estabelecido

Causas comuns:

```
Causa 199 (Nenhum recurso disponível):
  → Pool de IP esgotado
  → Verifique: curl http://pgw:9090/metrics | grep
address_registry_count
  → Expanda o pool de IP em ue.subnet_map

Causa 202 (IE obrigatório ausente):
  → SGSN não enviando IEs necessários
  → Verifique a configuração do SGSN
  → Revise a mensagem no tcpdump

Causa 204 (Falha do sistema):
  → Falha do UPF/PFCP
  → Verifique o status da associação PFCP
  → Revise os logs do OmniPGW
```

Problema: Falha na Atualização do Contexto PDP

Sintomas:

- Resposta de Atualização de Contexto PDP com causa de erro
- Handover falha

Causas possíveis:

- Contexto PDP não encontrado (TEID diferente)
- Incompatibilidade de NSAPI
- Sessão já excluída

Depuração:

```
# Verifique sessões ativas
curl http://pgw:9090/metrics | grep session_count

# Revise logs para busca de contexto
journalctl -u omnipgw | grep "PDP Context"
```

Melhores Práticas

Design de Rede

1. **Porta Compartilhada com S5/S8**
    - Gn e S5/S8 compartilham a porta UDP 2123
    - OmniPGW detecta automaticamente a versão GTP a partir da mensagem
    - Um único IP pode atender tanto 2G/3G quanto 4G
2. **Conectividade do SGSN**
    - Assegure que todos os SGSNs possam alcançar o IP do GGSN

- Considere VLAN dedicada para tráfego Gn
- Planeje para roaming (Gp) se aplicável

3. **Planejamento de Endereço IP**

- Os mesmos pools de IP atendem tanto os modos PGW quanto GGSN
- Considere pools baseados em APN separados para 2G/3G

Desempenho

1. **Capacidade de Sessão**

- Monitore a métrica `session_count`
- Planeje para o número esperado de assinantes 2G/3G
- Considere que 2G/3G geralmente tem menos sessões simultâneas

2. **Tamanhos de Buffer UDP**

- As mesmas recomendações que S5/S8
- Típico: 4-8 MB por socket

Considerações de Migração

Ao migrar de um GGSN autônomo para o OmniPGW:

1. **Configuração de APN**

- Assegure que os APNs correspondam à configuração existente do GGSN
- Verifique as configurações do servidor DNS em PCO

2. **Migração de Pool de IP**

- Planeje cuidadosamente a transição do pool de IP
- Considere migração gradual por APN

3. **Mapeamento de QoS**

- Perfis QoS R99 aceitos como estão
- Nenhuma tradução de QCI necessária para 2G/3G

Documentação Relacionada

Funções Centrais

- **Guia de Configuração** - Referência completa de configuração
- **Gerenciamento de Sessão** - Detalhes do ciclo de vida da sessão
- **Alocação de IP do UE** - Gerenciamento de endereços IP
- **Configuração PCO** - Opções de Configuração de Protocolo

Interfaces Relacionadas

- **Interface S5/S8** - Interface equivalente 4G/LTE
- **Interface PFCP** - Coordenação do plano de usuário
- **Interface Diameter Gy** - Cobrança online

Operações

- **Guia de Monitoramento** - Métricas e alertas
- **Solução de Problemas** - Problemas comuns
- **Formato de CDR de Dados** - Geração de CDR

Referências

- 3GPP TS 29.060 - Protocolo de Tunelamento GPRS (GTP) através da interface Gn e Gp
- 3GPP TS 23.060 - Serviço Geral de Pacote de Rádio (GPRS); Descrição do serviço
- 3GPP TS 24.008 - Especificação da Camada 3 da interface de rádio móvel (perfis QoS)

Voltar ao Índice da Documentação

Interface Gn/Gp do OmniPGW - *por Omnitouch Network Services*

Guia de Monitoramento e Métricas do OmniPGW

Integração com Prometheus e Monitoramento Operacional

por Omnitouch Network Services

Índice

Visão Geral

OmniPGW fornece duas abordagens complementares de monitoramento:

1. Interface Web em Tempo Real (coberta brevemente aqui, detalhada nos respectivos documentos da interface)

- Visualizador de sessão ao vivo
- Status do peer PFCP
- Conectividade do peer Diameter

- Inspeção de sessão individual

2. Métricas do Prometheus (foco principal deste documento)

- Tendências históricas e análise
- Alertas e notificações
- Métricas de performance
- Planejamento de capacidade

Este documento foca nas **métricas do Prometheus**. Para detalhes da Interface Web, veja:

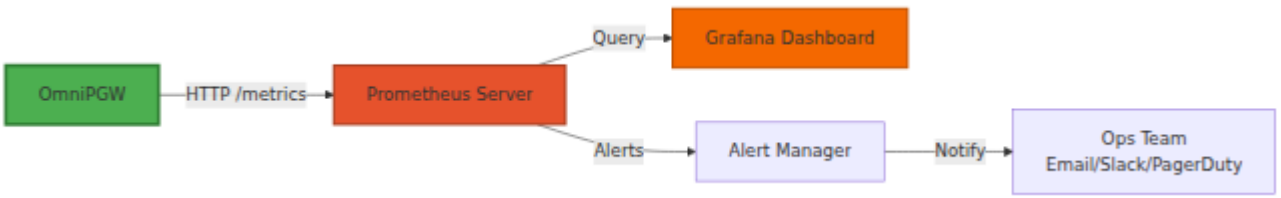
- Gerenciamento de Sessões - Interface Web
- Interface PFCP - Interface Web
- Diameter Gx - Interface Web

Visão Geral das Métricas do Prometheus

OmniPGW expõe **métricas compatíveis com Prometheus** para monitoramento abrangente da saúde do sistema, performance e capacidade. Isso permite que as equipes de operações:

- **Monitorar a Saúde do Sistema** - Acompanhar sessões ativas, alocações e erros
- **Planejamento de Capacidade** - Compreender tendências de utilização de recursos
- **Análise de Performance** - Medir a latência de manipulação de mensagens
- **Alertas** - Notificação proativa de problemas
- **Depuração** - Identificar causas raízes de problemas

Arquitetura de Monitoramento



Endpoint de Métricas

Configuração

Ative as métricas em `config/runtime.exs`:

```
config :pgw_c,
  metrics: %{
    enabled: true,
    ip_address: "0.0.0.0",  # Vincular a todas as interfaces
    port: 9090,              # Porta HTTP
    registry_poll_period_ms: 5_000  # Intervalo de polling
  }
```

Acessando Métricas

Endpoint HTTP:

```
http://<omnipgw_ip>:<port>/metrics
```

Exemplo:

```
curl http://10.0.0.20:9090/metrics
```

Formato de Saída

As métricas são expostas no **formato de texto do Prometheus**:

```
# HELP teid_registry_count The number of TEID registered to
sessions
# TYPE teid_registry_count gauge
teid_registry_count 150

# HELP address_registry_count The number of addresses registered
to sessions
# TYPE address_registry_count gauge
address_registry_count 150

# HELP s5s8_inbound_messages_total The total number of messages
received from S5/S8 peers
# TYPE s5s8_inbound_messages_total counter
s5s8_inbound_messages_total{message_type="create_session_request"}
1523
s5s8_inbound_messages_total{message_type="delete_session_request"}
1487
```

Métricas Disponíveis

OmniPGW expõe as seguintes categorias de métricas:

Métricas de Sessão

Contagens de Sessões Ativas:

Nome da Métrica	Tipo	Descrição
`teid_registry_count`	Gauge	Sessões S5/S8 ativas (contagem de TEID)
`seid_registry_count`	Gauge	Sessões PFCP ativas (contagem de SEID)
`session_id_registry_count`	Gauge	Sessões Gx ativas (contagem de Diameter Session-ID)
`session_registry_count`	Gauge	Sessões ativas (pares IMSI, EBI)
`address_registry_count`	Gauge	Endereços IP de UE alocados
`charging_id_registry_count`	Gauge	IDs de cobrança ativos (veja Formato de CDR de Dados para registros de cobrança CDR)
`sxb_sequence_number_registry_count`	Gauge	Respostas PFCP pendentes (aguardando resposta)
`s5s8_sequence_number_registry_count`	Gauge	Respostas S5/S8 pendentes (aguardando resposta)
`sxb_peer_registry_count`	Gauge	Número de processos de peer PFCP registrados

Uso:

```
# Sessões ativas atuais
teid_registry_count

# Taxa de criação de sessões (por segundo)
rate(teid_registry_count[5m])

# Sessões máximas na última hora
max_over_time(teid_registry_count[1h])
```

Contadores de Mensagens

Mensagens S5/S8 (GTP-C):

Nome da Métrica	Tipo	Rótulos	Descrição
`s5s8_inbound_messages_total`	Counter	`message_type`	Total de mensagens S5/S8 recebidas
`s5s8_outbound_messages_total`	Counter	`message_type`	Total de mensagens S5/S8 enviadas
`s5s8_inbound_errors_total`	Counter	`message_type`	Erros de processament S5/S8

Tipos de Mensagens:

- `create_session_request`
- `create_session_response`
- `delete_session_request`
- `delete_session_response`
- `create_bearer_request`

- `delete_bearer_request`

Mensagens Sxb (PFCP):

Nome da Métrica	Tipo	Rótulos	Descrição
`sxb_inbound_messages_total`	Counter	`message_type`	Total de mensagens PFCP recebidas
`sxb_outbound_messages_total`	Counter	`message_type`	Total de mensagens PFCP enviadas
`sxb_inbound_errors_total`	Counter	`message_type`	Erros de processamento PFCP recebidos
`sxb_outbound_errors_total`	Counter	`message_type`	Erros de processamento PFCP enviados

Tipos de Mensagens:

- `association_setup_request`
- `association_setup_response`
- `heartbeat_request`
- `heartbeat_response`
- `session_establishment_request`
- `session_establishment_response`
- `session_modification_request`
- `session_deletion_request`

Mensagens Gx (Diameter):

Nome da Métrica	Tipo	Rótulos	Descri
`gx_inbound_messages_total`	Counter	`message_type`	Total de mensage Diameter recebidas
`gx_outbound_messages_total`	Counter	`message_type`	Total de mensage Diameter enviadas
`gx_inbound_errors_total`	Counter	`message_type`	Erros de processar Diameter recebidos
`gx_outbound_errors_total`	Counter	`message_type`	Erros de processar Diameter enviados
`gx_outbound_responses_total`	Counter	`message_type`, `result_code_class`, `diameter_host`	Resposta Diameter enviadas categoriz por classe código de resultado host peer

Tipos de Mensagens:

- `gx_CCA` (Credit-Control-Answer)
- `gx_CCR` (Credit-Control-Request)
- `gx_RAA` (Re-Auth-Answer)
- `gx_RAR` (Re-Auth-Request)

Classes de Código de Resultado (para `gx_outbound_responses_total`):

- `2xxx` - Respostas de sucesso (ex: 2001 DIAMETER_SUCCESS)
- `3xxx` - Erros de protocolo (ex: 3001 DIAMETER_COMMAND_UNSUPPORTED)
- `4xxx` - Falhas transitórias (ex: 4001 DIAMETER_AUTHENTICATION_REJECTED)
- `5xxx` - Falhas permanentes (ex: 5012 DIAMETER_UNABLE_TO_COMPLY)

Exemplos de Uso:

```
# Monitorar taxa de sucesso de respostas Gx
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}[5m]))
sum(rate(gx_outbound_responses_total[5m])) * 100

# Rastrear falhas por host PCRF
rate(gx_outbound_responses_total{result_code_class!="2xxx"}[5m]) by (

# Contar total de mensagens Re-Auth-Answer bem-sucedidas
gx_outbound_responses_total{message_type="gx_RAA",result_code_class="

# Alertar sobre alta taxa de falhas para PCRF específico
rate(gx_outbound_responses_total{result_code_class=~"4xxx|5xxx",diame
[5m]) > 0.1
```

Tratamento de Erros:

Nome da Métrica	Tipo	Rótulos	Descrição
`rescues_total`	Counter	`module`, `function`	Total de blocos de resgate atingidos (tratamento de exceções)

Métricas de Latência

Duração do Processamento de Mensagens Recebidas:

Nome da Métrica	Tipo	Rótulos	
`s5s8_inbound_handling_duration`	Histogram	`request_message_type`	T r c r S c c e r
`sxb_inbound_handling_duration`	Histogram	`request_message_type`	T r c r P c c e r
`gx_inbound_handling_duration`	Histogram	`request_message_type`	T r c r D (c c e r

Duração de Transação de Saída:

Nome da Métrica	Tipo	Rótulos
`s5s8_outbound_transaction_duration`	Histogram	`request_message_type`
`sxb_outbound_transaction_duration`	Histogram	`request_message_type`
`gx_outbound_transaction_duration`	Histogram	`request_message_type`

Buckets (segundos):

- Valores: 0.0001, 0.0005, 0.001, 0.005, 0.01, 0.05, 0.1, 0.5, 1.0, 5.0
- (100µs, 500µs, 1ms, 5ms, 10ms, 50ms, 100ms, 500ms, 1s, 5s)

Uso:

```
# Latência S5/S8 do 95º percentil
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# Latência média PFCP
rate(sxb_inbound_handling_duration_sum[5m]) /
rate(sxb_inbound_handling_duration_count[5m])
```

Monitoramento de Saúde do UPF

Métricas de Peer UPF:

Nome da Métrica	Tipo	Rótulos	Descrição
`upf_peers_total`	Gauge	-	Total de peers UPF registrados
`upf_peers_healthy`	Gauge	-	Número de peers UPF saudáveis (associados + batimentos de coração OK)
`upf_peers_unhealthy`	Gauge	-	Número de peers UPF não saudáveis
`upf_peers_associated`	Gauge	-	Número de peers UPF com associação PFCP ativa
`upf_peers_unassociated`	Gauge	-	Número de peers UPF sem associação PFCP
`upf_peer_healthy`	Gauge	`peer_ip`	Status de saúde de um UPF específico (1=saudável, 0=não saudável)
`upf_peer_missed_heartbeats`	Gauge	`peer_ip`	Batimentos de coração consecutivos perdidos para um UPF específico

Uso:

```
# Monitorar saúde do pool UPF
upf_peers_healthy / upf_peers_total

# Alertar sobre UPFs não saudáveis
upf_peers_unhealthy > 0

# Rastrear saúde de um UPF específico
upf_peer_healthy{peer_ip="10.98.0.20"}

# Identificar UPFs com problemas de batimento de coração
upf_peer_missed_heartbeats > 2
```

Exemplos de Alertas:

```yaml
# Alertar quando UPF fica fora do ar
- alert: UPF_Peer_Down
  expr: upf_peer_healthy == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "UPF {{ $labels.peer_ip }} está fora do ar"
    description: "Peer UPF não respondendo aos batimentos de
coração PFCP"

# Alertar quando múltiplos UPFs estão fora do ar
- alert: UPF_Pool_Degraded
  expr: (upf_peers_healthy / upf_peers_total) < 0.5
  for: 2m
  labels:
    severity: critical
  annotations:
    summary: "Pool UPF degradado"
    description: "Apenas {{ $value | humanizePercentage }} dos
UPFs estão saudáveis"

# Aviso sobre batimentos de coração perdidos
- alert: UPF_Heartbeat_Issues
  expr: upf_peer_missed_heartbeats > 2
  for: 30s
  labels:
    severity: warning
  annotations:
    summary: "UPF {{ $labels.peer_ip }} com problemas de batimento
de coração"
    description: "{{ $value }} batimentos de coração consecutivos
perdidos"
```

Monitoramento de Saúde do P-CSCF

Métricas do Servidor P-CSCF:

Nome da Métrica	Tipo	Rótulos	Descrição
`pcscf_fqdns_total`	Gauge	-	Total de FQDNs P-CSCF sendo monitorados
`pcscf_fqdns_resolved`	Gauge	-	FQDNs P-CSCF resolvidos com sucesso via DNS
`pcscf_fqdns_failed`	Gauge	-	FQDNs P-CSCF que falharam na resolução DNS
`pcscf_servers_total`	Gauge	-	Total de servidores P-CSCF descobertos
`pcscf_servers_healthy`	Gauge	`fqdn`	Servidores P-CSCF saudáveis por FQDN
`pcscf_servers_unhealthy`	Gauge	`fqdn`	Servidores P-CSCF não saudáveis por FQDN

Veja: Guia de Monitoramento P-CSCF para rastreamento detalhado da saúde IMS.

Métricas de Licença

Status da Licença:

Nome da Métrica	Tipo	Descrição
`license_status`	Gauge	Status atual da licença (1 = válido, 0 = inválido)

Uso:

```
# Verificar se a licença é válida
license_status == 1

# Alertar sobre licença inválida
license_status == 0
```

Exemplo de Alerta:

```
- alert: PGW_C_License_Invalid
  expr: license_status == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "Licença PGW-C inválida ou expirada"
    description: "O status da licença é inválido - solicitações de
criação de sessão estão sendo bloqueadas"
```

Impacto da Licença Inválida:

Quando a licença é inválida ou o servidor de licença não está acessível, **Solicitações de Criação de Sessões serão rejeitadas** com o código de causa GTP-C **"Sem recursos disponíveis" (73)**. Isso é visível em capturas de pacotes como mostrado abaixo:

Captura do Wireshark mostrando Resposta de Criação de Sessão com causa "Sem recursos disponíveis" quando a licença é inválida

Notas:

- Nome do produto registrado com o servidor de licença: `omnipgwc`
- A URL do servidor de licença está configurada em `config/runtime.exs` sob `:license_client`
- Quando a licença é inválida (`license_status == 0`), solicitações de criação de sessão são bloqueadas com o código de causa GTP-C 73 (Sem recursos disponíveis)
- A interface do usuário e o monitoramento permanecem acessíveis independentemente do status da licença
- Peers Diameter, GTP-C e PFCP continuam a manter conexões
- Sessões existentes não são afetadas - apenas a criação de novas sessões é bloqueada

Métricas do Sistema

Métricas do VM Erlang:

Nome da Métrica	Tipo	Descrição
`vm_memory_total`	Gauge	Memória total da VM (bytes)
`vm_memory_processes`	Gauge	Memória usada pelos processos
`vm_memory_system`	Gauge	Memória usada pelo sistema
`vm_system_process_count`	Gauge	Total de processos Erlang
`vm_system_port_count`	Gauge	Total de portas abertas

Configuração do Prometheus

Configuração de Scrape

Adicione o OmniPGW ao `prometheus.yml` do Prometheus:

```yaml
# prometheus.yml
global:
  scrape_interval: 15s
  evaluation_interval: 15s

scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets: ['10.0.0.20:9090']
        labels:
          instance: 'omnipgw-01'
          environment: 'production'
          site: 'datacenter-1'
```

Múltiplas Instâncias do OmniPGW

```yaml
scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets:
          - '10.0.0.20:9090'
          - '10.0.0.21:9090'
          - '10.0.0.22:9090'
        labels:
          environment: 'production'
```

Descoberta de Serviço

Kubernetes:

```yaml
scrape_configs:
  - job_name: 'omnipgw'
    kubernetes_sd_configs:
      - role: pod
    relabel_configs:
      - source_labels: [__meta_kubernetes_pod_label_app]
        action: keep
        regex: omnipgw
      - source_labels: [__meta_kubernetes_pod_ip]
        target_label: __address__
        replacement: '${1}:9090'
```

Verificação

Teste de scrape:

```
# Verificar alvos do Prometheus
curl http://prometheus:9090/api/v1/targets

# Consultar uma métrica
curl 'http://prometheus:9090/api/v1/query?
query=teid_registry_count'
```

Painéis do Grafana

Configuração do Painel

1. Adicionar Fonte de Dados do Prometheus:

```
Configuração → Fontes de Dados → Adicionar fonte de dados →
Prometheus
URL: http://prometheus:9090
```

2. Importar Painel:

Crie um novo painel ou importe de JSON.

Painéis Principais

Painel 1: Sessões Ativas

```
# Consulta
teid_registry_count

# Tipo de Painel: Gauge
# Limiares:
#   Verde: < 5000
#   Amarelo: 5000-8000
#   Vermelho: > 8000
```

Painel 2: Taxa de Sessão

```
# Consulta
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])

# Tipo de Painel: Gráfico
# Unidade: solicitações/segundo
```

Painel 3: Utilização do Pool de IP

```
# Consulta (para sub-rede /24 com 254 IPs)
(address_registry_count / 254) * 100

# Tipo de Painel: Gauge
# Unidade: percentual (0-100)
# Limiares:
#   Verde: < 70%
#   Amarelo: 70-85%
#   Vermelho: > 85%
```

Painel 4: Latência de Mensagem (95º Percentil)

```
# Consulta
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)

# Tipo de Painel: Gráfico
# Unidade: milissegundos
```

Painel 5: Taxa de Erros

```
# Consulta
rate(s5s8_inbound_errors_total[5m])

# Tipo de Painel: Gráfico
# Unidade: erros/segundo
# Limite de Alerta: > 0.1
```

Painel 6: Taxa de Sucesso de Respostas Gx

```
# Consulta: Calcular percentual de respostas Gx bem-sucedidas
sum(rate(gx_outbound_responses_total{result_code_class="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Tipo de Painel: Gauge
# Unidade: percentual (0-100)
# Limiares:
#   Verde: > 95%
#   Amarelo: 90-95%
#   Vermelho: < 90%
```

Alternativa - Divisão por Classe de Código de Resultado:

```
# Consulta: Mostrar contagens de respostas por classe de código de
resultado
sum(rate(gx_outbound_responses_total[5m])) by (result_code_class)

# Tipo de Painel: Gráfico de Pizza ou Gráfico de Barras
# Legenda: {{ result_code_class }}
```

Alternativa - Status de Resposta por PCRF:

```
# Consulta: Mostrar respostas por host PCRF
sum(rate(gx_outbound_responses_total[5m])) by (diameter_host,
result_code_class)

# Tipo de Painel: Gráfico de Barras Empilhadas
# Legenda: {{ diameter_host }} - {{ result_code_class }}
```

Painel 7: Status de Saúde do UPF

```
# Consulta: Percentual geral de saúde do pool
(upf_peers_healthy / upf_peers_total) * 100

# Tipo de Painel: Gauge
# Unidade: percentual (0-100)
# Limiares:
#   Verde: 100%
#   Amarelo: 50-99%
#   Vermelho: < 50%
```

Alternativa - Status por UPF:

```
# Consulta: Saúde individual do UPF
upf_peer_healthy

# Tipo de Painel: Estatística
# Mapeamentos:
#   1 = "UP" (Verde)
#   0 = "DOWN" (Vermelho)
```

Exemplo Completo de Painel

```
{
  "dashboard": {
    "title": "OmniPGW - Painel de Operações",
    "panels": [
      {
        "title": "Sessões Ativas",
        "targets": [
          {
            "expr": "teid_registry_count",
            "legendFormat": "Sessões Ativas"
          }
        ],
        "type": "graph"
      },
      {
        "title": "Taxa de Criação de Sessões",
        "targets": [
          {
            "expr":
"rate(s5s8_inbound_messages_total{message_type=\"create_session_reque
[5m])",
            "legendFormat": "Sessões/segundo"
          }
        ],
        "type": "graph"
      },
      {
        "title": "Utilização do Pool de IP",
        "targets": [
          {
            "expr": "(address_registry_count / 254) * 100",
            "legendFormat": "Uso do Pool %"
          }
        ],
        "type": "gauge"
      },
      {
        "title": "Latência de Mensagem (p95)",
        "targets": [
          {
            "expr": "histogram_quantile(0.95,
```

```
rate(s5s8_inbound_handling_duration_bucket[5m]))",
            "legendFormat": "S5/S8 p95"
          },
          {
            "expr": "histogram_quantile(0.95,
rate(sxb_inbound_handling_duration_bucket[5m]))",
            "legendFormat": "PFCP p95"
          }
        ],
        "type": "graph"
      }
    ]
  }
}
```

Alertas

Regras de Alerta

Crie `omnipgw_alerts.yml`:

```yaml
groups:
  - name: omnipgw
    interval: 30s
    rules:
      # Alertas de Contagem de Sessões
      - alert: OmniPGW_HighSessionCount
        expr: teid_registry_count > 8000
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Contagem de sessões alta no OmniPGW"
          description: "{{ $value }} sessões ativas (limite:
8000)"

      - alert: OmniPGW_SessionCountCritical
        expr: teid_registry_count > 9500
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Contagem de sessões crítica no OmniPGW"
          description: "{{ $value }} sessões ativas se aproximando
da capacidade"

      # Alertas de Pool de IP
      - alert: OmniPGW_IPPoolUtilizationHigh
        expr: (address_registry_count / 254) * 100 > 80
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Utilização alta do pool de IP no OmniPGW"
          description: "Pool de IP {{ $value }}% utilizado"

      - alert: OmniPGW_IPPoolExhausted
        expr: address_registry_count >= 254
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Pool de IP esgotado no OmniPGW"
          description: "Nenhum IP disponível para alocação"
```

```
      # Alertas de Taxa de Erros
      - alert: OmniPGW_HighErrorRate
        expr: rate(s5s8_inbound_errors_total[5m]) > 0.1
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta taxa de erros no OmniPGW"
          description: "{{ $value }} erros/segundo na interface
S5/S8"

      - alert: OmniPGW_GxErrorRate
        expr: rate(gx_inbound_errors_total[5m]) > 0.05
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Erros Gx no OmniPGW"
          description: "{{ $value }} erros Diameter/segundo"

      # Alertas de Respostas Gx
      - alert: OmniPGW_GxResponseFailureRate
        expr: |

sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
          sum(rate(gx_outbound_responses_total[5m])) > 0.1
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta taxa de falhas de resposta Gx no OmniPGW"
          description: "{{ $value | humanizePercentage }} das
respostas Gx são falhas (códigos de resultado não-2xxx)"

      - alert: OmniPGW_GxPCRFFailures
        expr:
rate(gx_outbound_responses_total{result_code_class=~"4xxx|5xxx"}
[5m]) by (diameter_host) > 0.05
        for: 3m
        labels:
          severity: warning
        annotations:
```

```
          summary: "PCRF {{ $labels.diameter_host }} recebendo
respostas de falha"
          description: "{{ $value }} respostas de falha/segundo
para PCRF {{ $labels.diameter_host }}"

      # Alertas de Saúde do UPF
      - alert: OmniPGW_UPF_PeerDown
        expr: upf_peer_healthy == 0
        for: 1m
        labels:
          severity: critical
        annotations:
          summary: "Peer UPF {{ $labels.peer_ip }} fora do ar"
          description: "UPF não respondendo aos batimentos de
coração PFCP"

      - alert: OmniPGW_UPF_PoolDegraded
        expr: (upf_peers_healthy / upf_peers_total) < 0.5
        for: 2m
        labels:
          severity: critical
        annotations:
          summary: "Pool UPF degradado"
          description: "{{ $value | humanizePercentage }} dos UPFs
estão saudáveis (< 50%)"

      - alert: OmniPGW_UPF_HeartbeatFailures
        expr: upf_peer_missed_heartbeats > 2
        for: 30s
        labels:
          severity: warning
        annotations:
          summary: "UPF {{ $labels.peer_ip }} falhas de batimento
de coração"
          description: "{{ $value }} batimentos de coração
consecutivos perdidos"

      - alert: OmniPGW_UPF_AllDown
        expr: upf_peers_healthy == 0 and upf_peers_total > 0
        for: 30s
        labels:
          severity: critical
        annotations:
          summary: "Todos os peers UPF fora do ar"
```

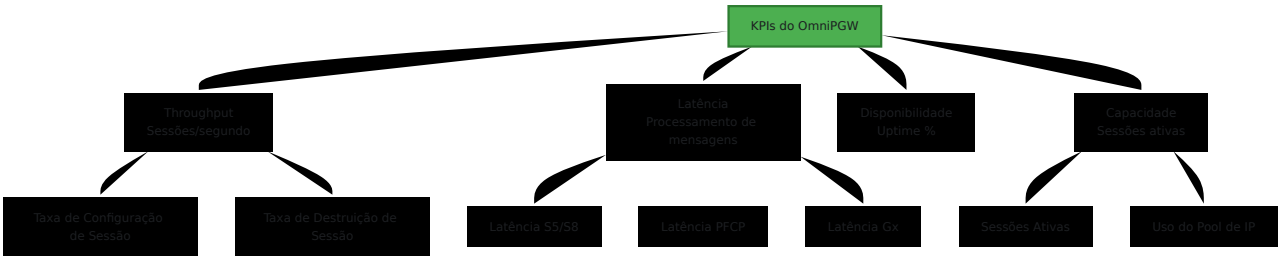
```
          description: "Nenhum UPF saudável disponível para
criação de sessão"

      # Alertas de Latência
      - alert: OmniPGW_HighLatency
        expr: |
          histogram_quantile(0.95,
            rate(s5s8_inbound_handling_duration_bucket[5m])
          ) > 100000
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "Alta latência de mensagem no OmniPGW"
          description: "Latência p95 {{ $value }}µs (> 100ms)"

      # Alertas do Sistema
      - alert: OmniPGW_HighMemoryUsage
        expr: vm_memory_total > 2000000000
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Alta utilização de memória no OmniPGW"
          description: "VM utilizando {{ $value | humanize }}B de
memória"

      - alert: OmniPGW_HighProcessCount
        expr: vm_system_process_count > 100000
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "Alta contagem de processos no OmniPGW"
          description: "{{ $value }} processos Erlang (possível
vazamento)"
```

Configuração do AlertManager

```yaml
# alertmanager.yml
global:
  resolve_timeout: 5m

route:
  receiver: 'ops-team'
  group_by: ['alertname', 'instance']
  group_wait: 10s
  group_interval: 10s
  repeat_interval: 12h

  routes:
    - match:
        severity: critical
      receiver: 'pagerduty'

    - match:
        severity: warning
      receiver: 'slack'

receivers:
  - name: 'ops-team'
    email_configs:
      - to: 'ops@example.com'

  - name: 'slack'
    slack_configs:
      - api_url:
'https://hooks.slack.com/services/YOUR/SLACK/WEBHOOK'
        channel: '#omnipgw-alerts'
        title: 'Alerta OmniPGW: {{ .GroupLabels.alertname }}'
        text: '{{ range .Alerts }}{{ .Annotations.description }}{{
end }}'

  - name: 'pagerduty'
    pagerduty_configs:
      - service_key: 'YOUR_PAGERDUTY_KEY'
```

Monitoramento de Performance

Indicadores-Chave de Performance (KPIs)



Consultas de Throughput

Taxa de Configuração de Sessão:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])
```

Taxa de Destruição de Sessão:

```
rate(s5s8_inbound_messages_total{message_type="delete_session_request
[5m])
```

Crescimento Líquido de Sessões:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m]) -
rate(s5s8_inbound_messages_total{message_type="delete_session_request
[5m])
```

Análise de Latência

Latência de Processamento de Mensagens (Percentis):

```
# p50 (Mediana)
histogram_quantile(0.50,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# p95
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# p99
histogram_quantile(0.99,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)
```

Divisão de Latência por Tipo de Mensagem:

```
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
) by (request_message_type)
```

Tendência de Capacidade

Tendência de Crescimento de Sessões (24h):

```
teid_registry_count -
teid_registry_count offset 24h
```

Capacidade Restante:

```
# Para capacidade máxima de 10.000 sessões
10000 - teid_registry_count
```

Tempo até o Esgotamento da Capacidade:

```
# Dias até a capacidade esgotada (com base na taxa de crescimento
de 1h)
(10000 - teid_registry_count) /
(rate(teid_registry_count[1h]) * 86400)
```

Solução de Problemas com Métricas

Identificando Problemas

Problema: Alta Taxa de Rejeição de Sessões

Consulta:

```
rate(s5s8_inbound_errors_total[5m]) by (message_type)
```

Ação:

- Verifique os logs de erro
- Verifique a conectividade do PCRF (erros Gx)
- Verifique o esgotamento do pool de IP

Problema: Configuração de Sessão Lenta

Consulta:

```
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Ação:

- Verifique a latência Gx (tempo de resposta do PCRF)
- Verifique a latência PFCP (tempo de resposta do PGW-U)
- Revise o uso de recursos do sistema

Problema: Falhas de Política do PCRF

Consultas:

```
# Taxa geral de falhas de resposta Gx
sum(rate(gx_outbound_responses_total{result_code_class!="2xxx"}
[5m])) /
sum(rate(gx_outbound_responses_total[5m])) * 100

# Divisão por host PCRF
sum(rate(gx_outbound_responses_total[5m])) by (diameter_host,
result_code_class)

# Classes de código de resultado específicas
rate(gx_outbound_responses_total{result_code_class="5xxx"}[5m]) by
(diameter_host)
```

Ação:

- Verifique a conectividade e saúde do PCRF
- Revise os perfis de assinantes no PCRF (erros 5xxx geralmente indicam problemas de política)
- Verifique a configuração do peer Diameter
- Verifique os logs do PCRF para erros correspondentes
- Para 5012 (DIAMETER_UNABLE_TO_COMPLY), revise o manuseio de Re-Auth-Request

Problema: Vazamento de Memória Suspeito

Consultas:

```
# Tendência de memória total
rate(vm_memory_total[1h])

# Tendência de memória do processo
rate(vm_memory_processes[1h])

# Tendência de contagem de processos
rate(vm_system_process_count[1h])
```

Ação:

- Verifique se há sessões obsoletas
- Revise as contagens de registro
- Reinicie se o vazamento for confirmado

Consultas de Depuração

Encontrar Hora de Pico de Sessão:

```
max_over_time(teid_registry_count[24h])
```

Comparar Atual vs. Histórico:

```
teid_registry_count /
avg_over_time(teid_registry_count[7d])
```

Identificar Anomalias:

```
abs(
  teid_registry_count -
  avg_over_time(teid_registry_count[1h])
) > 100
```

Melhores Práticas

Coleta de Métricas

1. **Intervalo de Scrape:** 15-30 segundos (equilibrar granularidade vs. carga)
2. **Retenção:** 15+ dias para análise histórica
3. **Rótulos:** Use rotulagem consistente (instância, ambiente, site)

Design de Painéis

1. **Painel de Visão Geral** - KPIs de alto nível para NOC
2. **Painéis Detalhados** - Análise profunda por interface
3. **Painel de Solução de Problemas** - Métricas de erro e logs

Design de Alertas

1. **Evitar Fadiga de Alertas** - Alertar apenas sobre problemas acionáveis
2. **Escalonamento** - Aviso → Crítico com gravidade crescente
3. **Contexto** - Incluir links de runbook nas descrições de alerta

---

Documentação Relacionada

Configuração e Configuração

- **Guia de Configuração** - Configuração de métricas do Prometheus, configuração da Interface Web
- **Guia de Solução de Problemas** - Usando métricas para depuração

Métricas de Interface

- **Interface PFCP** - Métricas de sessão PFCP, monitoramento de saúde do UPF

- **Interface Diameter Gx** - Métricas de política Gx, rastreamento de interação com PCRF
- **Interface Diameter Gy** - Métricas de cobrança Gy, rastreamento de cotas, timeouts de OCS
- **Interface S5/S8** - Métricas de mensagens GTP-C, comunicação SGW-C

Monitoramento Especializado

- **Monitoramento P-CSCF** - Métricas de descoberta P-CSCF, saúde IMS
- **Gerenciamento de Sessões** - Sessões ativas, métricas do ciclo de vida da sessão
- **Alocação de IP de UE** - Métricas de utilização do pool de IP

Voltar ao Guia de Operações

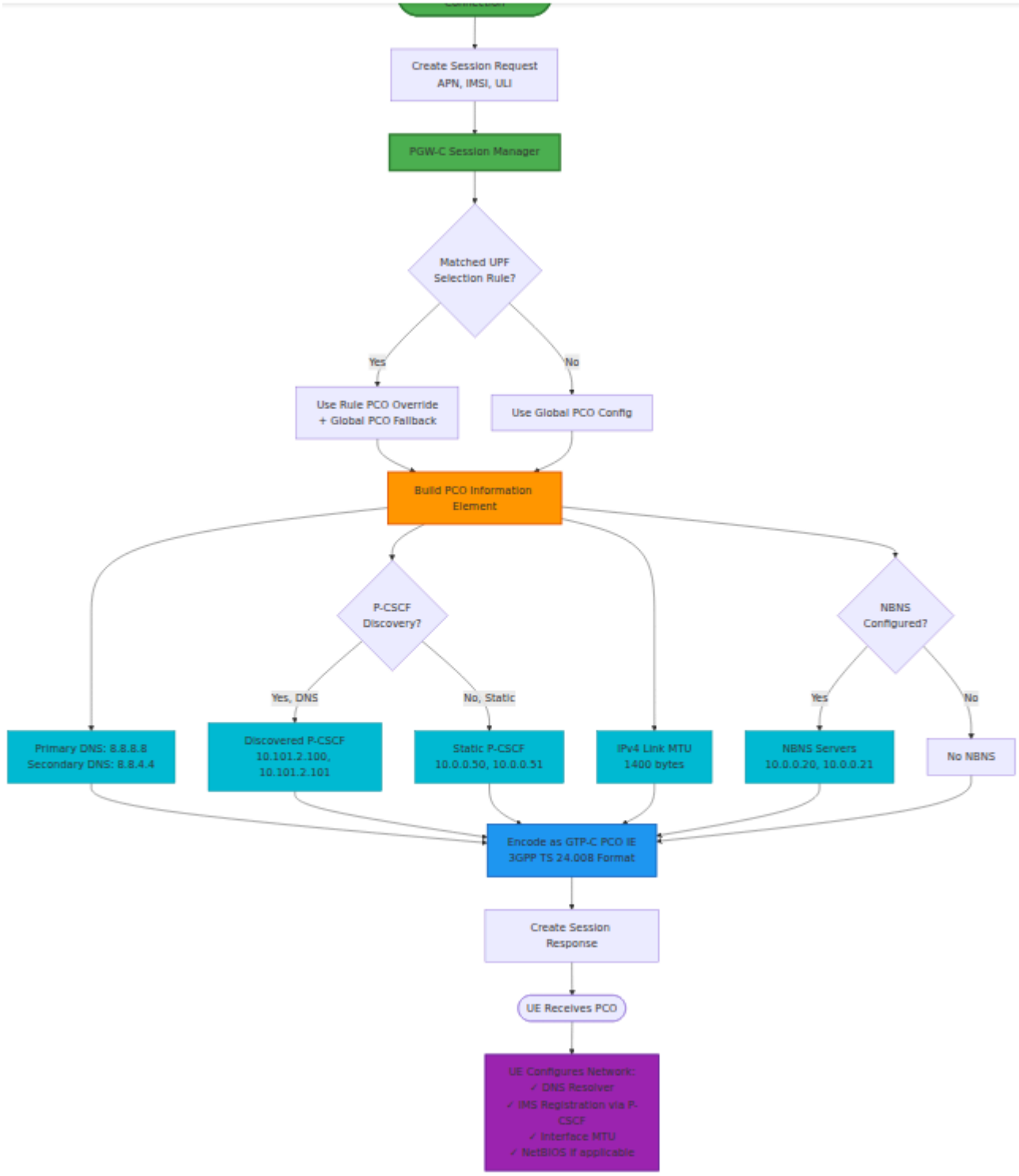
Opções de Configuração de Protocolo (PCO)

Parâmetros de Rede Entregues ao UE

OmniPGW da Omnitouch Network Services

Visão Geral

PCO (Opções de Configuração de Protocolo) são parâmetros de rede enviados ao UE (dispositivo móvel) durante o estabelecimento da conexão PDN. Esses parâmetros permitem que o UE acesse serviços de rede como DNS, IMS e configure as configurações de rede.



Elementos de Informação PCO:

Nome do IE	ID do Contêiner	Descrição	Necessário
Endereço IPv4 do Servidor DNS	0x000D	DNS Primário	Sim
Endereço IPv4 do Servidor DNS	0x000D	DNS Secundário	Opcional
Endereço IPv4 do P-CSCF	0x000C	P-CSCF para IMS	Opcional (IMS)
MTU do Link IPv4	0x0010	Unidade máxima de transmissão	Recomendado
Endereço IPv4 do Servidor NBNS	0x0011	Servidor de nome NetBIOS	Opcional

---

Configuração

Configuração Básica

```
# config/runtime.exs
config :pgw_c,
  pco: %{
    # Servidores DNS (obrigatório)
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",

    # Servidores NBNS (opcional, para dispositivos Windows)
    primary_nbns_server_address: nil,
    secondary_nbns_server_address: nil,

    # Endereços P-CSCF para IMS/VoLTE (opcional)
    p_cscf_ipv4_address_list: [],

    # Descoberta Dinâmica de P-CSCF (opcional)
    p_cscf_discovery_enabled: false,
    p_cscf_discovery_dns_server: nil,
    p_cscf_discovery_timeout_ms: 5000,

    # Tamanho MTU IPv4 (bytes)
    ipv4_link_mtu_size: 1400
  }
```

Parâmetros PCO

Endereços de Servidor DNS

DNS Primário e Secundário:

```
pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}
```

Provedores de DNS Comuns:

Provedor	Primário	Secundário
Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

DNS Privado:

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11"
}
```

Endereços P-CSCF (IMS)

Para Serviços IMS/VoLTE:

```
pco: %{
  p_cscf_ipv4_address_list: [
    "10.0.0.50",  # P-CSCF Primário
    "10.0.0.51"   # P-CSCF Secundário
  ]
}
```

P-CSCF (Função de Controle de Sessão de Chamada Proxy):

- Ponto de entrada para sinalização IMS
- Necessário para VoLTE, VoWiFi, RCS
- UE utiliza SIP através deste servidor

Descoberta Dinâmica de P-CSCF

Descoberta P-CSCF Baseada em DNS:

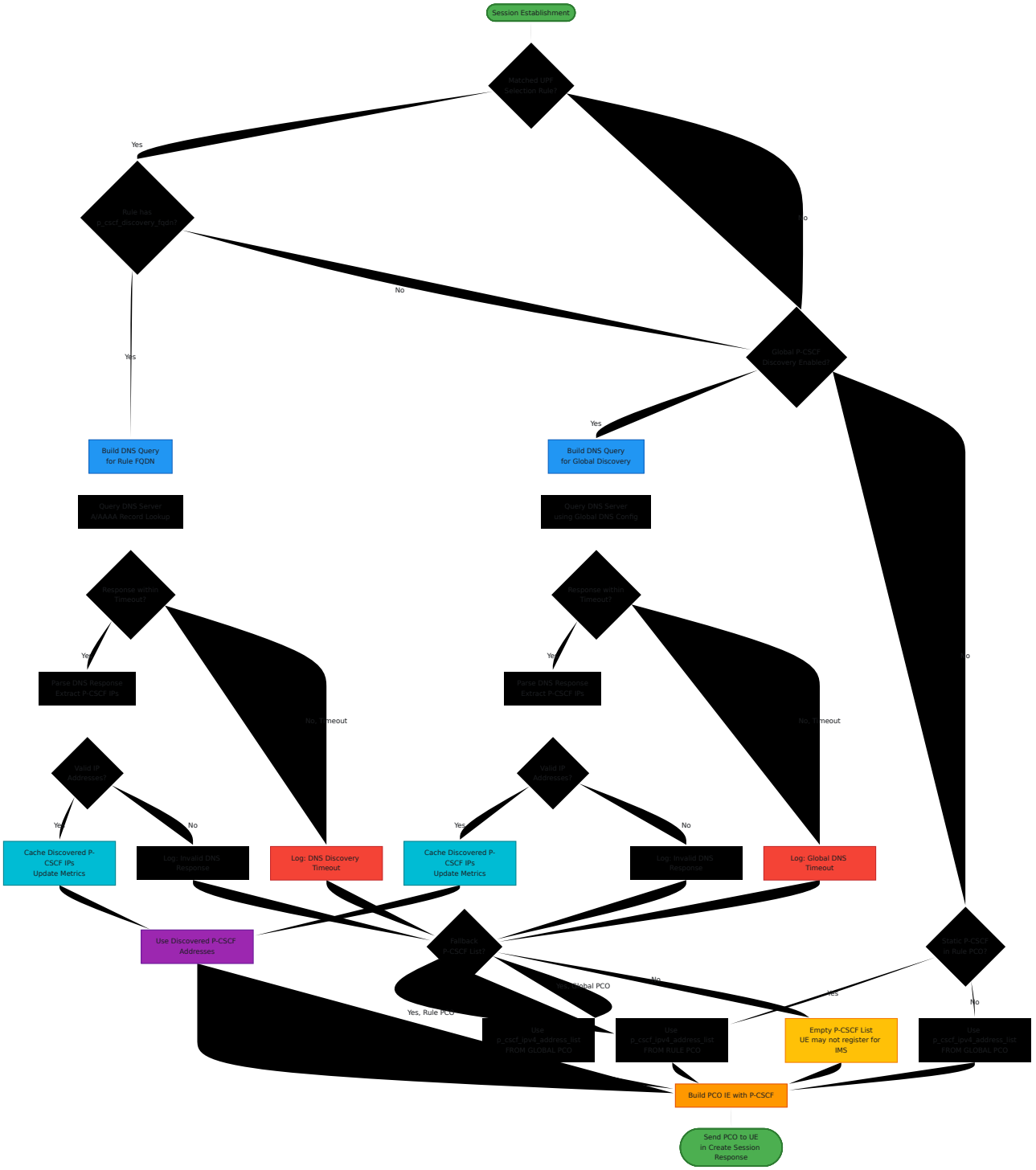
OmniPGW suporta descoberta dinâmica de P-CSCF via consultas DNS conforme definido nas 3GPP TS 23.003 e TS 24.229. Quando habilitado, o PGW-C pode consultar o DNS para endereços P-CSCF em vez de usar configuração estática.

```
pco: %{
  # Habilitar descoberta dinâmica de P-CSCF
  p_cscf_discovery_enabled: true,

  # Servidor DNS para consultas P-CSCF (como tupla)
  p_cscf_discovery_dns_server: {10, 179, 2, 177},

  # Timeout para consultas DNS (milissegundos)
  p_cscf_discovery_timeout_ms: 5000,

  # Lista estática de P-CSCF (usada como fallback se o DNS falhar)
  p_cscf_ipv4_address_list: ["10.0.0.50"]
}
```

Como Funciona:

1. Quando `p_cscf_discovery_enabled: true`, o PGW-C realiza consultas DNS para endereços P-CSCF
2. A consulta DNS é enviada para o `p_cscf_discovery_dns_server` configurado
3. Se a consulta DNS for bem-sucedida, os endereços P-CSCF descobertos são enviados ao UE via PCO
4. Se a consulta DNS falhar ou expirar, recai para a lista estática `p_cscf_ipv4_address_list`
5. Veja Monitoramento P-CSCF para monitoramento detalhado e métricas

Fluxo de Descoberta P-CSCF



Prioridade de Descoberta:

1. **Descoberta FQDN por Regra** (Maior Prioridade) - `p_cscf_discovery_fqdn` na regra de seleção UPF
2. **Descoberta DNS Global** - `p_cscf_discovery_enabled: true` na configuração global de PCO

3. **Lista Estática de PCO por Regra** - `p_cscf_ipv4_address_list` na sobreposição de PCO por regra
4. **Lista Estática de PCO Global** (Fallback) - `p_cscf_ipv4_address_list` na configuração global de PCO

Monitoramento:

Todas as tentativas de descoberta de P-CSCF são registradas e acompanhadas com métricas:

- Taxas de sucesso/falha de consulta DNS
- Latência de descoberta
- Estatísticas de uso de fallback
- Métricas de descoberta por regra e global

Veja Monitoramento P-CSCF para detalhes completos de monitoramento.

Opções de Configuração:

Parâmetro	Tipo	Padrão	Descrição
`p_cscf_discovery_enabled`	Booleano	`false`	Habilitar descoberta dinâmica de P-CSCF baseada em DNS
`p_cscf_discovery_dns_server`	Tupla (IP)	`nil`	Endereço IP do servidor DNS como tupla 4 (por exemplo, `{10, 179, 2, 177}`)
`p_cscf_discovery_timeout_ms`	Inteiro	`5000`	Timeout para consultas DNS em milissegundos

Casos de Uso:

- **Implantações IMS dinâmicas** - Endereços P-CSCF mudam com base na configuração DNS
- **Balanceamento de carga geográfica** - DNS retorna os servidores P-CSCF mais próximos
- **Alta disponibilidade** - DNS retorna automaticamente servidores P-CSCF disponíveis
- **Ambientes multi-inquilinos** - Diferentes assinantes recebem diferentes servidores P-CSCF

Exemplo: IMS de Produção com Descoberta DNS

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",

  # Habilitar descoberta dinâmica de P-CSCF
  p_cscf_discovery_enabled: true,
  p_cscf_discovery_dns_server: {10, 179, 2, 177},  # Servidor DNS
IMS
  p_cscf_discovery_timeout_ms: 3000,

  # Endereços P-CSCF de fallback (se o DNS falhar)
  p_cscf_ipv4_address_list: [
    "10.0.0.50",  # Fallback primário
    "10.0.0.51"   # Fallback secundário
  ],

  ipv4_link_mtu_size: 1400
}
```

Descoberta P-CSCF por Regra:

A descoberta P-CSCF também pode ser configurada por regra de seleção UPF. Isso permite que diferentes APNs usem diferentes servidores DNS para descoberta de P-CSCF:

```
# Na configuração de seleção upf
rules: [
  %{
    name: "IMS Traffic",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [...],

    # Descoberta P-CSCF por regra
    p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org"
  }
]
```

Veja Configuração de Seleção UPF para detalhes sobre descoberta P-CSCF por regra.

Veja também: Monitoramento P-CSCF para monitoramento da descoberta e saúde do P-CSCF

Servidores NBNS (NetBIOS)

Para Compatibilidade com Dispositivos Windows:

```
pco: %{
  primary_nbns_server_address: "10.0.0.20",
  secondary_nbns_server_address: "10.0.0.21"
}
```

Quando Usar:

- Redes empresariais com dispositivos Windows
- Suporte a aplicativos legados
- Resolução de nomes NetBIOS necessária

Tamanho MTU do Link

Unidade Máxima de Transmissão:

```
pco: %{
  ipv4_link_mtu_size: 1400  # bytes
}
```

Valores MTU Comuns:

MTU	Caso de Uso
1500	Ethernet padrão (sem tunelamento)
1400	Sobrecarga de tunelamento GTP contabilizada
1420	Sobrecarga reduzida
1280	MTU mínima IPv6
1360	Ambientes VPN/túnel

Recomendação: Use **1400** para LTE para contabilizar a sobrecarga de GTP-U.

Exemplos de Configuração

APN de Internet

```
pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4",
  ipv4_link_mtu_size: 1400
}
```

APN IMS

```
pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11",
  p_cscf_ipv4_address_list: [
    "10.0.0.50",
    "10.0.0.51"
  ],
  ipv4_link_mtu_size: 1400
}
```

Veja: Monitoramento P-CSCF para monitoramento das taxas de sucesso de registro IMS e saúde do P-CSCF

APN Empresarial

```
pco: %{
  primary_dns_server_address: "10.100.0.10",
  secondary_dns_server_address: "10.100.0.11",
  primary_nbns_server_address: "10.100.0.20",
  secondary_nbns_server_address: "10.100.0.21",
  ipv4_link_mtu_size: 1400
}
```

PCO em Mensagens GTP-C

Resposta de Criação de Sessão

OmniPGW inclui PCO na mensagem **Resposta de Criação de Sessão**:

```
Create Session Response
├── Cause: Request accepted
├── UE IP Address: 100.64.1.42
├── PCO (Protocol Configuration Options)
│   ├── DNS Server IPv4 Address: 8.8.8.8
│   ├── DNS Server IPv4 Address: 8.8.4.4
│   ├── P-CSCF IPv4 Address: 10.0.0.50
│   ├── P-CSCF IPv4 Address: 10.0.0.51
│   └── IPv4 Link MTU: 1400
```

Processamento do UE

O UE recebe PCO e:

1. Configura o resolvedor DNS com os servidores fornecidos
2. Registra-se no P-CSCF para serviços IMS
3. Define o MTU da interface para o valor especificado

Solução de Problemas

Problema: UE Não Consegue Resolver DNS

Sintomas:

- UE tem endereço IP, mas não consegue acessar a internet
- Consultas DNS falham

Causas Possíveis:

1. Endereços de servidor DNS incorretos na configuração PCO
2. Servidores DNS não acessíveis a partir do pool de IP do UE
3. Firewall bloqueando o tráfego DNS

Resolução:

```
# Testar a acessibilidade do servidor DNS
ping 8.8.8.8

# Testar a resolução DNS a partir da rede UE
nslookup google.com 8.8.8.8

# Verificar a configuração PCO
grep "primary_dns_server_address" config/runtime.exs
```

Problema: Falha no Registro IMS

Sintomas:

- Chamadas VoLTE falham
- UE mostra "Sem registro IMS"

Causas Possíveis:

1. Configuração P-CSCF ausente
2. Endereços IP do P-CSCF incorretos
3. P-CSCF não acessível

Resolução:

```
# Verificar a configuração P-CSCF
pco: %{
  p_cscf_ipv4_address_list: ["10.0.0.50"]  # Garantir que não
esteja vazio
}
```

Problema: Problemas de MTU

Sintomas:

- Alguns sites carregam, outros não
- Transferências de arquivos grandes falham
- Problemas de fragmentação

Causas Possíveis:

- MTU muito grande para a sobrecarga de tunelamento
- MTU muito pequeno causando fragmentação excessiva

Resolução:

```
# Recomendado: 1400 para tunelamento GTP
pco: %{
  ipv4_link_mtu_size: 1400
}

# Se ainda houver problemas, tente um valor menor
pco: %{
  ipv4_link_mtu_size: 1360
}
```

Melhores Práticas

Configuração de DNS

1. **Use Servidores DNS Confiáveis**
    - Público: Google (8.8.8.8), Cloudflare (1.1.1.1)
    - Privado: DNS interno para empresas
2. **Sempre Configure Secundário**
    - Fornece redundância
    - Melhora a confiabilidade
3. **Considere a Segurança do DNS**
    - Resolvedores compatíveis com DNSSEC
    - Filtragem de DNS para segurança

Configuração IMS

1. **Forneça Múltiplos P-CSCF**
    - Pelo menos 2 para redundância
    - Distribuição geográfica, se possível
2. **Garanta Acessibilidade**
    - O P-CSCF deve ser acessível a partir do pool de IP do UE
    - Testar conectividade SIP

Otimização de MTU

1. **Contabilize a Sobrecarga**
    - GTP-U: 36 bytes (IPv4)
    - IPsec: Variável (50-100 bytes)
2. **MTU Padrão para LTE**
    - Recomendado: **1400 bytes**
    - Equilibra throughput e compatibilidade
3. **Teste de Ponto a Ponto**
    - Descoberta de MTU de caminho
    - Testar com pacotes grandes

Documentação Relacionada

Guias de Configuração

- **Guia de Configuração** - Referência completa do runtime.exs, seleção UPF com sobreposições de PCO
- **Alocação de IP do UE** - Gerenciamento de pool de IP, alocação baseada em APN

- **Monitoramento P-CSCF** - Monitoramento da descoberta P-CSCF, rastreamento de saúde, métricas

Gerenciamento de Sessão e Interface

- **Gerenciamento de Sessão** - Ciclo de vida da sessão PDN, estabelecimento de bearer
- **Interface S5/S8** - Protocolo GTP-C, codificação e entrega de PCO
- **Interface PFCP** - Estabelecimento de sessão do plano do usuário

IMS e VoLTE

- **Interface Diameter Gx** - Controle de política para bearers IMS
- **Guia de Monitoramento** - Métricas e painéis relacionados ao PCO

Voltar ao Guia de Operações

Descoberta e Monitoramento do P-CSCF

Descoberta Dinâmica do Servidor P-CSCF com Monitoramento em Tempo Real

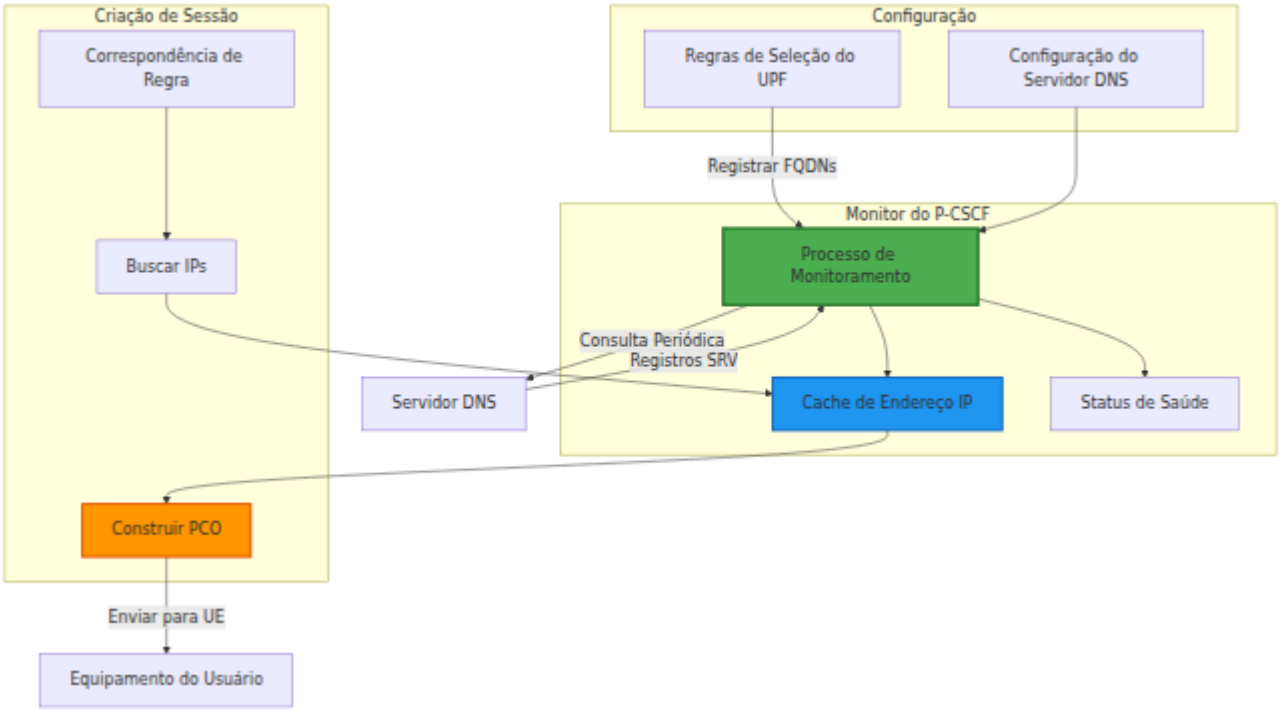
OmniPGW da Omnitouch Network Services

Visão Geral

Descoberta e Monitoramento do P-CSCF (Função de Controle de Sessão de Chamada Proxy) fornece descoberta dinâmica de servidores IMS P-CSCF usando consultas DNS SRV com verificação de saúde SIP OPTIONS em tempo real. Este recurso permite:

- **Descoberta do P-CSCF por Regra**: Diferentes servidores P-CSCF para diferentes tipos de tráfego
- **Monitoramento Automático**: Processo em segundo plano monitora continuamente a resolução DNS (a cada 60 segundos)
- **Verificações de Saúde SIP OPTIONS**: Verifica se os servidores P-CSCF estão ativos via pings SIP OPTIONS
  - **TCP Primeiro**: Tenta SIP OPTIONS via TCP (preferido pela confiabilidade)
  - **Fallback UDP**: Retorna para UDP se o TCP falhar
  - **Rastreamento de Status**: Marca cada servidor como :up ou :down com base na resposta
- **Rastreamento de Saúde em Tempo Real**: A interface da Web exibe o status de resolução, IPs descobertos e status de saúde
- **Fallback Elegante**: Estratégia de fallback em três camadas para máxima confiabilidade

- **Métricas Prometheus**: Total observabilidade via métricas Prometheus



Índice

Introdução Rápida

Configuração Básica

```
# config/runtime.exs

# Configuração global do PCO (servidor DNS para descoberta do P-
CSCF)
config :pgw_c,
  pco: %{
    p_cscf_discovery_dns_server: "10.179.2.177",
    p_cscf_discovery_enabled: true,
    p_cscf_discovery_timeout_ms: 5000
  },

  upf_selection: %{
    rules: [
      # Tráfego IMS - Descoberta dinâmica do P-CSCF
      %{
        name: "Tráfego IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80}
        ],
        # FQDN de Descoberta do P-CSCF (veja o Guia de
Configuração para mais regras de seleção do UPF)
        p_cscf_discovery_fqdn:
"pcscf.mnc380.mcc313.3gppnetwork.org",
        # Fallback estático (veja o Guia de Configuração do PCO)
        pco: %{
          p_cscf_ipv4_address_list: ["10.101.2.100",
"10.101.2.101"]
        }
      }
    ]
  }
```

Veja o Guia de Configuração para a configuração completa da regra de seleção do UPF e Configuração do PCO para opções de fallback estático do P-CSCF.

Monitoramento de Acesso

1. Inicie o OmniPGW
2. Navegue até **Interface da Web → Monitor do P-CSCF** (`https://localhost:8086/pcscf_monitor`)
3. Veja o status de resolução em tempo real e os IPs descobertos

---

Configuração

Configurações Globais de Descoberta do P-CSCF

Configure o servidor DNS usado para a descoberta do P-CSCF na seção PCO:

```
pco: %{
  # Servidor DNS para descoberta do P-CSCF (separado do DNS
fornecido ao UE)
  p_cscf_discovery_dns_server: "10.179.2.177",

  # Habilitar recurso de descoberta DNS do P-CSCF
  p_cscf_discovery_enabled: true,

  # Tempo limite para consultas DNS SRV (milissegundos)
  p_cscf_discovery_timeout_ms: 5000,

  # Endereços P-CSCF estáticos (fallback global)
  p_cscf_ipv4_address_list: ["10.101.2.146"]
}
```

FQDNs do P-CSCF por Regra

Cada regra de seleção do UPF pode especificar seu próprio FQDN de descoberta do P-CSCF:

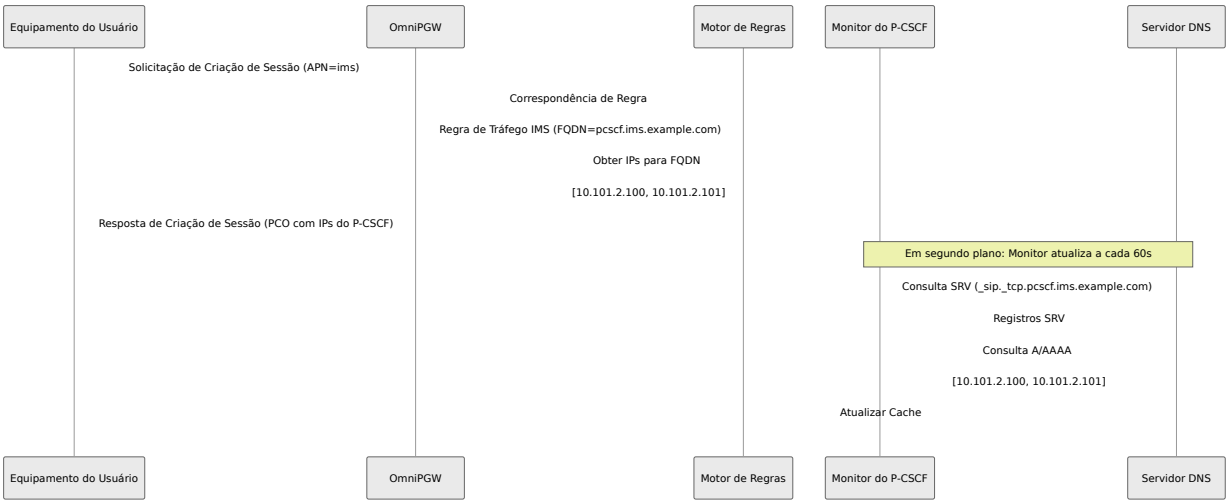
```
upf_selection: %{
  rules: [
    # Tráfego IMS - P-CSCF específico do IMS
    %{
      name: "Tráfego IMS",
      match_field: :apn,
      match_regex: "^ims",
      upf_pool: [...],
      p_cscf_discovery_fqdn:
"pcscf.ims.mnc380.mcc313.3gppnetwork.org",
      pco: %{
        p_cscf_ipv4_address_list: ["10.101.2.100"]  # Fallback
      }
    },

    # Empresa - P-CSCF específico da empresa
    %{
      name: "Tráfego Empresarial",
      match_field: :apn,
      match_regex: "^enterprise",
      upf_pool: [...],
      p_cscf_discovery_fqdn: "pcscf.enterprise.example.com",
      pco: %{
        p_cscf_ipv4_address_list: ["192.168.1.50"]  # Fallback
      }
    },

    # Internet - Sem descoberta do P-CSCF (usa configuração
global)
    %{
      name: "Tráfego da Internet",
      match_field: :apn,
      match_regex: "^internet",
      upf_pool: [...]
      # Sem p_cscf_discovery_fqdn - usa configuração global do PCO
    }
  ]
}
```

Como Funciona

Processo de Inicialização

1. **Aplicação Inicia**
    - O GenServer do Monitor do P-CSCF é inicializado
    - O analisador de configuração extrai todos os FQDNs únicos do P-CSCF das regras de seleção do UPF
2. **Registro de FQDN**
    - Cada FQDN único é registrado no monitor
    - O monitor realiza a consulta inicial de DNS SRV para cada FQDN
    - **Verificação de Saúde SIP OPTIONS** (em paralelo para todos os servidores descobertos):
        - Tente TCP primeiro (`SIP/2.0/TCP` na porta 5060)
        - Se o TCP falhar, retorne para UDP (`SIP/2.0/UDP` na porta 5060)
        - Marque cada servidor como `:up` (responde) ou `:down` (sem resposta/tempo esgotado)
    - Resultados (IPs, status de saúde ou erros) são armazenados em cache com timestamps
3. **Monitoramento Periódico** (A cada 60 segundos)
    - O monitor atualiza todos os FQDNs
    - Consultas DNS são executadas em segundo plano sem bloquear
    - Para cada servidor descoberto:
        - Envie SIP OPTIONS via TCP (tempo limite: 5 segundos)
        - Se o TCP falhar, tente UDP (tempo limite: 5 segundos)
        - Atualize o status de saúde com base na resposta
    - O cache é atualizado com os últimos resultados DNS e status de saúde

Fluxo de Criação de Sessão



Processo de Consulta DNS

O monitor usa **registros DNS SRV** para descoberta direta do P-CSCF:

1. **Consulta SRV**: Consulta registros SRV em `_sip._tcp.{fqdn}`
2. **Ordenação por Prioridade**: Ordena por prioridade e peso
3. **Extração de Alvo**: Extrai nomes de host dos registros SRV
4. **Resolução de Nome de Host**: Resolve nomes de host de destino para endereços IP (registros A/AAAA)
5. **Cache**: Armazena IPs resolvidos com status e timestamp

Precedência de Seleção de Endereço do P-CSCF

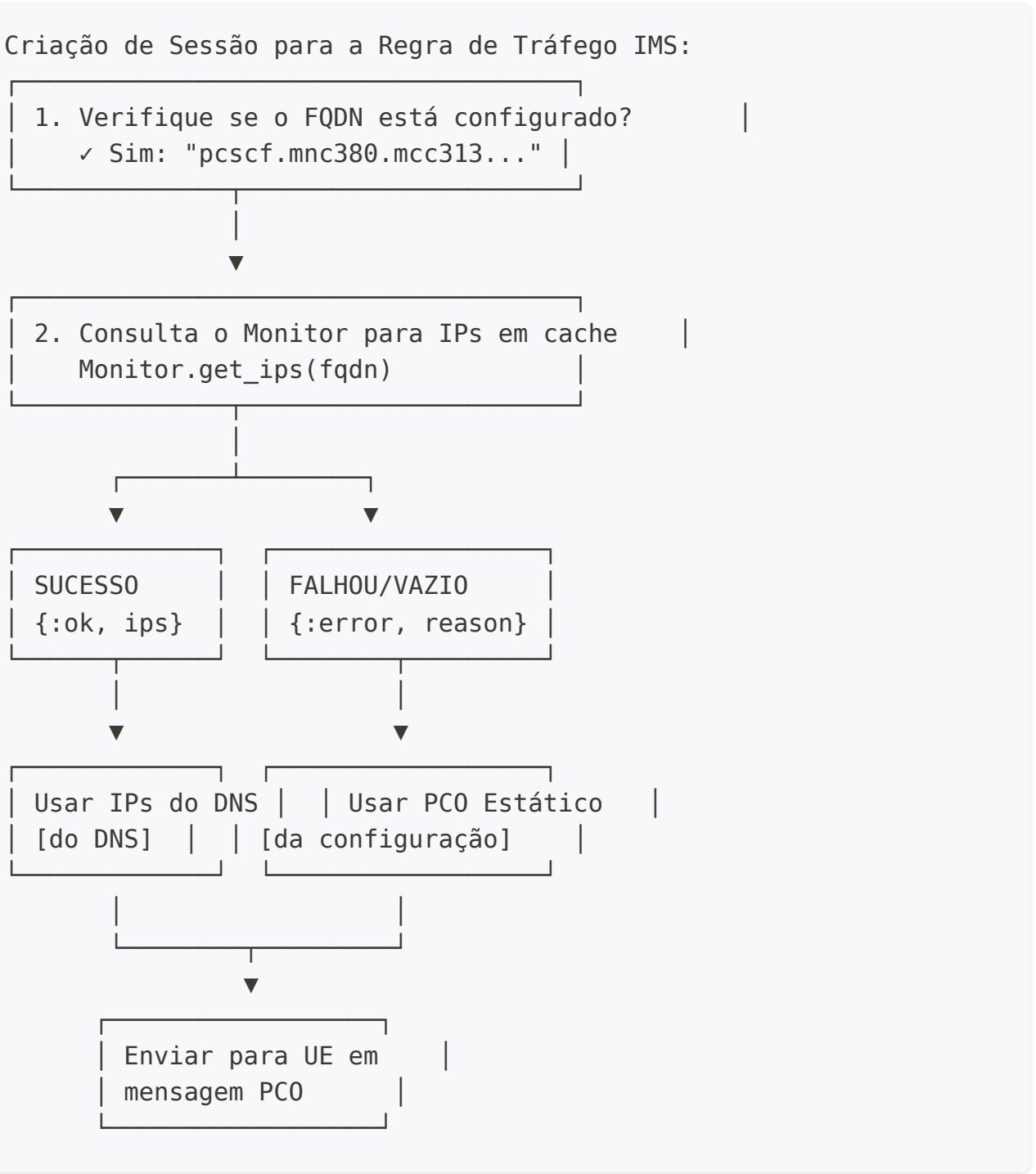
Quando tanto FQDN quanto PCO estático estão configurados em uma regra, o FQDN tem precedência:

```
%{
  name: "Tráfego IMS",
  p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org",  #
← Tentado PRIMEIRO
  pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]   #
← Fallback
  }
}
```

Lógica de Seleção:

Condição	Fonte do P-CSCF	IPs Usados	Mensagem
FQDN resolve com sucesso	Descoberta DNS (Monitor)	IPs descobertos do DNS	`"Usando en do P-CSCF pcscf.exam`
FQDN falha ao resolver	Sobrescrita do PCO da Regra	IPs estáticos de `pco.p_cscf_ipv4_address_list`	`"Falha ao IPs do P-C FQDN..., retornando configuraç estática"`
FQDN retorna lista vazia	Sobrescrita do PCO da Regra	IPs estáticos de `pco.p_cscf_ipv4_address_list`	Fallback aci
Monitor indisponível	Sobrescrita do PCO da Regra	IPs estáticos de `pco.p_cscf_ipv4_address_list`	Erro aciona
Nenhum FQDN configurado	Sobrescrita do PCO da Regra ou Global	IPs estáticos da regra ou configuração global	Usa configu estática dire

Fluxo de Exemplo:



Cenários do Mundo Real:

Cenário 1: Descoberta DNS Funciona

```
Config:
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  pco.p_cscf_ipv4_address_list: ["10.101.2.100"]

Resultado DNS: [10.101.2.150, 10.101.2.151]
UE Recebe: [10.101.2.150, 10.101.2.151] ← Do DNS
Nota: O PCO estático é ignorado quando o DNS tem sucesso
```

Cenário 2: DNS Falha, Fallback Elegante ⚠

```
Config:
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  pco.p_cscf_ipv4_address_list: ["10.101.2.100"]

Resultado DNS: ERRO :no_naptr_records
UE Recebe: [10.101.2.100] ← Do PCO estático
Nota: A sessão tem sucesso apesar da falha do DNS
```

Cenário 3: Nenhum FQDN Configurado

```
Config:
  # Nenhum p_cscf_discovery_fqdn
  pco.p_cscf_ipv4_address_list: ["192.168.1.50"]

UE Recebe: [192.168.1.50] ← Do PCO estático
Nota: Descoberta DNS não foi tentada
```

Por que este design?

1. **Preferir Dinâmico**: O DNS fornece flexibilidade, balanceamento de carga e roteamento ciente da localização
2. **Garantir Confiabilidade**: O fallback estático garante que as sessões nunca falhem devido a problemas de DNS
3. **Zero Intervenção Manual**: Failover automático sem envolvimento do operador
4. **Seguro para Produção**: O melhor dos dois mundos - agilidade com estabilidade

Recomendação: Sempre configure tanto o FQDN quanto o PCO estático para implantações em produção:

```
# ✓ RECOMENDADO: Dinâmico com fallback
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com",  # Preferido
  pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.100"]     # Rede de
segurança
  }
}

# ⚠ ARRISCADO: Apenas dinâmico (retorna para o PCO global)
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  # Sem fallback específico da regra!
}

# ✓ VÁLIDO: Apenas estático (sem sobrecarga de DNS)
%{
  pco: %{
    p_cscf_ipv4_address_list: ["192.168.1.50"]
  }
}
```

Monitoramento da Interface da Web

Página do Monitor do P-CSCF

Acesse a interface de monitoramento em: `https://localhost:8086/pcscf_monitor`

Recursos:

- **Estatísticas Gerais**
  - Total de FQDNs monitorados
  - FQDNs resolvidos com sucesso
  - Resoluções falhadas
  - Total de IPs do P-CSCF descobertos
- **Tabela de FQDN**
  - FQDN sendo monitorado
  - Status de resolução (✓ Resolvido / ✗ Falhou / □ Pendente)
  - Número de IPs descobertos
  - Lista de endereços IP resolvidos (com detalhes do servidor expansíveis)
  - Timestamp da última atualização
  - Botão de atualização manual por FQDN
  - **Status de Saúde**: Cada servidor descoberto mostra:
    - Endereço IP e porta
    - Nome do host (do alvo DNS SRV)
    - Indicador de saúde em tempo real (✓ Ativo / ✗ Inativo)

- **Controles de Atualização**
  - Botão **Atualizar Tudo**: Aciona reconsulta imediata de todos os FQDNs
  - **Atualização por FQDN**: Atualiza FQDNs individuais sob demanda
  - Atualização automática: Página atualiza a cada 5 segundos
- **Painel de Métricas de Monitoramento**
  - **Total de FQDNs**: Número de FQDNs únicos registrados para monitoramento
  - **Resolvidos com Sucesso**: FQDNs que foram resolvidos com sucesso via DNS
  - **Resoluções DNS Falhadas**: FQDNs que falharam ao resolver
  - **Total de Servidores P-CSCF**: Total de servidores descobertos em todos os FQDNs
  - ✓ **Saudáveis (SIP OPTIONS ATIVOS)**: Servidores respondendo a verificações de saúde SIP OPTIONS
  - ✗ **Não Saudáveis (SIP OPTIONS INATIVOS)**: Servidores não respondendo a SIP OPTIONS
  - **Taxa de Sucesso do DNS**: Porcentagem de resoluções DNS bem-sucedidas
  - **Intervalo de Verificação de Saúde**: Frequência das verificações de saúde SIP OPTIONS (60s, 5s de tempo limite)

O painel de métricas fornece visibilidade em tempo real sobre a saúde da resolução DNS e a disponibilidade do servidor P-CSCF via SIP OPTIONS.

Integração da Página de Seleção do UPF

A página de Seleção do UPF (`/upf_selection`) exibe o status de descoberta do P-CSCF para cada regra:

```
 Tráfego IMS (Prioridade 20)
   Correspondência: APN correspondente a ^ims
   Pool: UPF-IMS-Primário (10.100.2.21:8805)

    Descoberta do P-CSCF
      FQDN: pcscf.mnc380.mcc313.3gppnetwork.org
      Status: ✓ Resolvido (2 IPs)
      IPs Resolvidos: 10.101.2.100, 10.101.2.101

   ⚙ Sobrescritas do PCO
      DNS Primário: 10.103.2.195
      P-CSCF (fallback estático): 10.101.2.100, 10.101.2.101
```

Métricas e Observabilidade

Métricas Prometheus

O sistema de monitoramento do P-CSCF expõe métricas via Prometheus (porta 42069 por padrão):

Métricas de Gauge

```
# Métricas a nível de FQDN
pcscf_fqdns_total                       # Total de FQDNs
monitorados
pcscf_fqdns_resolved                    # FQDNs resolvidos com
sucesso (DNS teve sucesso)
pcscf_fqdns_failed                      # Resoluções de FQDN
falhadas (DNS falhou)

# Métricas a nível de servidor (agregado)
pcscf_servers_total                     # Total de servidores P-
CSCF descobertos via DNS SRV
pcscf_servers_healthy                   # Servidores respondendo a
SIP OPTIONS (agregado)
pcscf_servers_unhealthy                 # Servidores não
respondendo a SIP OPTIONS (agregado)

# Métricas a nível de servidor (por FQDN com rótulo)
pcscf_servers_healthy{fqdn="..."}      # Servidores saudáveis para
FQDN específico
pcscf_servers_unhealthy{fqdn="..."}    # Servidores não saudáveis
para FQDN específico
```

Detalhes da Verificação de Saúde:

- `healthy`: Servidor respondeu ao ping SIP OPTIONS (TCP ou UDP)
- `unhealthy`: Servidor não respondeu ao SIP OPTIONS (tempo limite de 5s por transporte)

Exemplos de Métricas

Métricas de Resolução DNS:

```
# Consultar FQDNs resolvidos com sucesso
pcscf_fqdns_resolved

# Calcular taxa de sucesso do DNS
(pcscf_fqdns_resolved / pcscf_fqdns_total) * 100

# Total de servidores descobertos
pcscf_servers_total
```

Métricas de Saúde SIP OPTIONS:

```
# Total de servidores saudáveis em todos os FQDNs
pcscf_servers_healthy

# Total de servidores não saudáveis
pcscf_servers_unhealthy

# Calcular taxa de sucesso da verificação de saúde
(pcscf_servers_healthy / pcscf_servers_total) * 100

# Servidores saudáveis para um FQDN específico
pcscf_servers_healthy{fqdn="pcscf.mnc380.mcc313.3gppnetwork.org"}

# Alerta quando todos os servidores estão inativos
pcscf_servers_healthy == 0 AND pcscf_servers_total > 0
```

Exemplos de Alertas Prometheus:

```yaml
# Alerta quando todos os servidores P-CSCF estão inativos
- alert: AllPCSCFServersDown
  expr: pcscf_servers_healthy == 0 AND pcscf_servers_total > 0
  for: 5m
  labels:
    severity: critical
  annotations:
    summary: "Todos os servidores P-CSCF estão não saudáveis"
    description: "{{ $value }} servidores saudáveis (0) - todos
falharam nas verificações SIP OPTIONS"

# Alerta quando mais de 50% dos servidores estão inativos
- alert: MajorityPCSCFServersDown
  expr: (pcscf_servers_healthy / pcscf_servers_total) < 0.5
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Maioria dos servidores P-CSCF estão não saudáveis"
    description: "Apenas {{ $value }}% dos servidores estão
respondendo a SIP OPTIONS"

# Alerta sobre falhas de resolução DNS
- alert: PCSCFDNSResolutionFailed
  expr: pcscf_fqdns_failed > 0
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Falhas de resolução DNS do P-CSCF"
    description: "{{ $value }} FQDN(s) falhando ao resolver"
```

Registro

O monitor registra eventos-chave:

```
[info] Monitor do P-CSCF iniciado
[info] Registrando 2 FQDNs únicos do P-CSCF para monitoramento:
["pcscf.ims.example.com", "pcscf.enterprise.example.com"]
[info] Monitor do P-CSCF: Registrando FQDN pcscf.ims.example.com
[debug] Monitor do P-CSCF: Resolvido com sucesso
pcscf.ims.example.com para 2 IPs
[warning] Monitor do P-CSCF: Falha ao resolver
pcscf.enterprise.example.com: :nxdomain
[debug] Usando endereços do P-CSCF do FQDN pcscf.ims.example.com:
[{10, 101, 2, 100}, {10, 101, 2, 101}]
```

Estratégia de Fallback

O sistema utiliza uma **estratégia de fallback em três camadas** para máxima confiabilidade:

Camada 1: Descoberta DNS (Preferida)

```
p_cscf_discovery_fqdn: "pcscf.ims.example.com"
```

- O monitor consulta o DNS e armazena os IPs resolvidos em cache
- A sessão usa IPs em cache se disponíveis
- **Vantagem**: Dinâmico, balanceado por carga, ciente da localização

Camada 2: PCO Estático Específico da Regra (Fallback)

```
pco: %{
  p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
}
```

- Usado se a descoberta DNS falhar ou não retornar IPs
- Configuração estática específica da regra

- **Vantagem**: Fallback específico da regra, previsível

Camada 3: Configuração Global do PCO (Último Recurso)

```
# Configuração global do pco
pco: %{
  p_cscf_ipv4_address_list: ["10.101.2.146"]
}
```

- Usado se não houver configuração específica da regra e o DNS falhar
- Endereços P-CSCF padrão global
- **Vantagem**: Sempre disponível, previne falha de sessão

Exemplo de Lógica de Fallback

```
A sessão corresponde à regra "Tráfego IMS":

1. Tente a descoberta DNS para "pcscf.ims.example.com"
   ├─ Sucesso → Usar [10.101.2.100, 10.101.2.101] ✓
   └─ Falha → Tente a próxima camada

2. Tente a sobrescrita do PCO da regra
   ├─── Configurado → Usar [10.101.2.100, 10.101.2.101] ✓
   └─ Não configurado → Tente a próxima camada

3. Use a configuração global do PCO
   └─ Usar [10.101.2.146] ✓ (Sempre tem sucesso)
```

Configuração DNS

Configuração do Servidor DNS

Configure o servidor DNS com registros SRV e A/AAAA para descoberta do P-CSCF:

```
; Registros SRV para P-CSCF (_sip._tcp prefix é consultado
automaticamente)
_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. IN SRV 10 50 5060
pcscf1.example.com.
_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. IN SRV 20 50 5060
pcscf2.example.com.

; Registros A
pcscf1.example.com. IN A 10.101.2.100
pcscf2.example.com. IN A 10.101.2.101
```

Importante: O OmniPGW automaticamente adiciona `_sip._tcp.` ao FQDN configurado. Se você configurar `p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org"`, o sistema consultará `_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org`.

Formato do Registro SRV

Os registros SRV seguem este formato:

```
_serviço._proto.domínio. IN SRV prioridade peso porta alvo.
```

- **Prioridade**: Valores mais baixos têm maior prioridade (10 antes de 20)
- **Peso**: Para balanceamento de carga entre a mesma prioridade (maior = mais tráfego)
- **Porta**: Porta SIP (tipicamente 5060 para TCP, 5060 para UDP)
- **Alvo**: Nome do host a ser resolvido para o endereço IP

Testando a Configuração DNS

```
# Consultar registros SRV (observe o prefixo _sip._tcp)
dig SRV _sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org
@10.179.2.177

# Saída esperada:
# _sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. 300 IN SRV 10 50
5060 pcscf1.example.com.

# Resolver nome do P-CSCF para IP
dig A pcscf1.example.com @10.179.2.177

# Saída esperada:
# pcscf1.example.com. 300 IN A 10.101.2.100
```

Solução de Problemas

Problema: FQDN Mostra Status "Falhou"

Sintomas:

- A interface da Web mostra status ✗ Falhou
- Erro: `:nxdomain`, `:timeout` ou `:no_naptr_records`

Possíveis Causas:

1. Servidor DNS não acessível
2. FQDN não existe no DNS
3. Nenhum registro NAPTR configurado
4. Tempo limite do servidor DNS

Resolução:

```
# 1. Testar conectividade do servidor DNS
ping 10.179.2.177

# 2. Testar consulta NAPTR manualmente
dig NAPTR pcscf.mnc380.mcc313.3gppnetwork.org @10.179.2.177

# 3. Verificar logs do OmniPGW
grep "P-CSCF" /var/log/pgw_c.log

# 4. Verificar configuração
grep "p_cscf_discovery_dns_server" config/runtime.exs

# 5. Atualização manual na interface da web
# Clique no botão "Atualizar" ao lado do FQDN falhado
```

Problema: Nenhum IP Retornado

Sintomas:

- A interface da Web mostra "0 IPs"
- O status pode ser ✓ Resolvido ou ✗ Falhou

Possíveis Causas:

1. Registros NAPTR existem, mas FQDNs de substituição não resolvem
2. Campo de serviço não corresponde ao padrão IMS/SIP
3. Registros A/AAAA ausentes

Resolução:

```
# Verificar campo de serviço do registro NAPTR
dig NAPTR pcscf.example.com @10.179.2.177

# Garantir que o serviço contenha "SIP" ou "IMS":
# CORRETO: "SIP+D2U", "x-3gpp-ims:sip"
# ERRADO: "HTTP", "FTP"

# Verificar se registros A/AAAA existem
dig pcscf1.example.com A @10.179.2.177
```

Problema: Sessões Usam o P-CSCF Errado

Sintomas:

- UE recebe endereços P-CSCF inesperados
- Fallback estático usado em vez de IPs descobertos

Possíveis Causas:

1. Descoberta DNS falhou, mas o fallback está funcionando
2. Correspondência de regra incorreta
3. FQDN não registrado

Resolução:

```
# 1. Verificar página do Monitor do P-CSCF
# Verificar se o FQDN está registrado e resolvido

# 2. Verificar logs da sessão
grep "Usando endereços do P-CSCF do FQDN" /var/log/pgw_c.log

# 3. Verificar página de Seleção do UPF
# Verificar se a regra mostra o FQDN correto e o status

# 4. Testar correspondência de regra
# Criar sessão com APN específico e verificar qual regra
corresponde
```

Problema: Alta Latência de Consulta DNS

Sintomas:

- Criação de sessão lenta
- Métricas mostram alta `pcscf_discovery_query_duration_seconds`

Possíveis Causas:

1. Problemas de desempenho do servidor DNS
2. Latência de rede para o servidor DNS

3. Tempo limite muito alto

Resolução:

```
# Reduzir tempo limite da consulta
pco: %{
  p_cscf_discovery_timeout_ms: 2000  # Reduzir de 5000ms
}

# Considerar usar servidor DNS mais próximo
pco: %{
  p_cscf_discovery_dns_server: "10.0.0.10"  # DNS local
}
```

Melhores Práticas

1. Seleção do Servidor DNS

Use Servidor DNS Dedicado

```
pco: %{
  # DNS dedicado para descoberta do P-CSCF (não o mesmo que o DNS
do UE)
  p_cscf_discovery_dns_server: "10.179.2.177",

  # Servidores DNS do UE (fornecidos aos dispositivos móveis)
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}
```

Por quê?

- Separar preocupações: DNS do UE vs. DNS interno do IMS
- Políticas de acesso e segurança diferentes
- Escalabilidade e confiabilidade independentes

2. Sempre Configure Fallback Estático

```
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com",  # Preferido
  pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.100"]  # Fallback
necessário
  }
}
```

Por quê?

- Garante que as sessões tenham sucesso mesmo se o DNS falhar
- Degradação elegante
- Atende aos requisitos de SLA

3. Use FQDNs Específicos por Tipo de Tráfego

```
rules: [
  # IMS
  %{
    name: "IMS",
    match_regex: "^ims",
    p_cscf_discovery_fqdn:
"pcscf.ims.mnc380.mcc313.3gppnetwork.org"
  },

  # Empresa
  %{
    name: "Empresa",
    match_regex: "^enterprise",
    p_cscf_discovery_fqdn: "pcscf.enterprise.example.com"
  }
]
```

Por quê?

- Diferentes pools de P-CSCF por serviço
- Melhor distribuição de carga

- Roteamento específico do serviço

4. Monitore o Desempenho da Consulta DNS

```
# Alerta sobre alta latência de consulta do P-CSCF
alert: HighPCSCFQueryLatency
expr: histogram_quantile(0.95,
pcscf_discovery_query_duration_seconds_bucket) > 2
for: 5m
labels:
  severity: warning
annotations:
  summary: "Consultas DNS do P-CSCF estão lentas (p95 > 2s)"
```

5. Verificações de Saúde DNS Regulares

- **Interface da Web**: Verifique a página do Monitor do P-CSCF diariamente
- **Métricas**: Monitore a métrica `pcscf_monitor_fqdns_failed`
- **Logs**: Fique atento a erros de DNS
- **Testes**: Verifique periodicamente se os registros DNS existem

6. Configure um Tempo Limite Apropriado

```
# Produção: Equilibrar confiabilidade vs. latência
pco: %{
  p_cscf_discovery_timeout_ms: 5000  # 5 segundos
}

# Alto desempenho: Favor velocidade, confiar no fallback
pco: %{
  p_cscf_discovery_timeout_ms: 2000  # 2 segundos
}
```

7. Use Redundância DNS

Configure DNS primário e secundário:

```
# DNS Primário do P-CSCF
pcscf.mnc380.mcc313.3gppnetwork.org. IN NAPTR 10 50 "s" "SIP+D2U"
"" _sip._udp.pcscf1.example.com.

# DNS Secundário do P-CSCF
pcscf.mnc380.mcc313.3gppnetwork.org. IN NAPTR 20 50 "s" "SIP+D2U"
"" _sip._udp.pcscf2.example.com.
```

Documentação Relacionada

- **Configuração do PCO** - Opções de Configuração de Protocolo, configurações de DNS e P-CSCF
- **Guia de Configuração** - Referência completa de configuração do OmniPGW
- **Monitoramento** - Métricas, registro e observabilidade
- **Gerenciamento de Sessão** - Ciclo de vida da sessão e entrega do PCO
- **Interface PFCP** - Comunicação da Função de Usuário

Voltar à Documentação Principal

Documentação da Interface PFCP/Sxb

Protocolo de Controle de Encaminhamento de Pacotes - Comunicação entre PGW-C e PGW-U

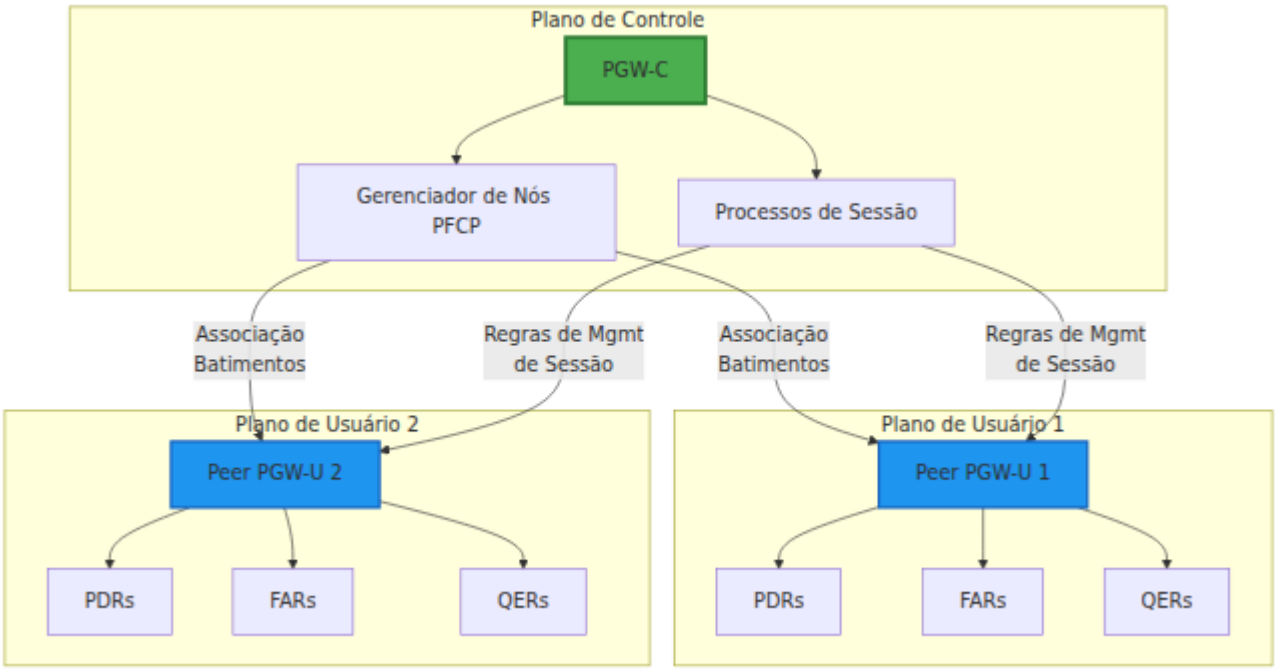
Índice

Visão Geral

A **interface Sxb** utiliza o **PFCP (Protocolo de Controle de Encaminhamento de Pacotes)** para comunicação entre o PGW-C (plano de controle) e o PGW-U (plano de usuário). Essa separação permite:

- **Plano de Controle (PGW-C)** - Gerencia sinalização, gerenciamento de sessão, decisões de política
- **Plano de Usuário (PGW-U)** - Gerencia o encaminhamento real de pacotes em alta velocidade

Arquitetura PFCP



Fundamentos do Protocolo

Versão PFCP

O PGW-C implementa a **Versão PFCP 1** (3GPP TS 29.244).

Transporte

- **Protocolo:** UDP
- **Porta Padrão:** 8805
- **Formato da Mensagem:** Codificado em binário usando a especificação PFCP

Tipos de ID de Nó

Os pares PFCP são identificados pelo ID do Nó, que pode ser:

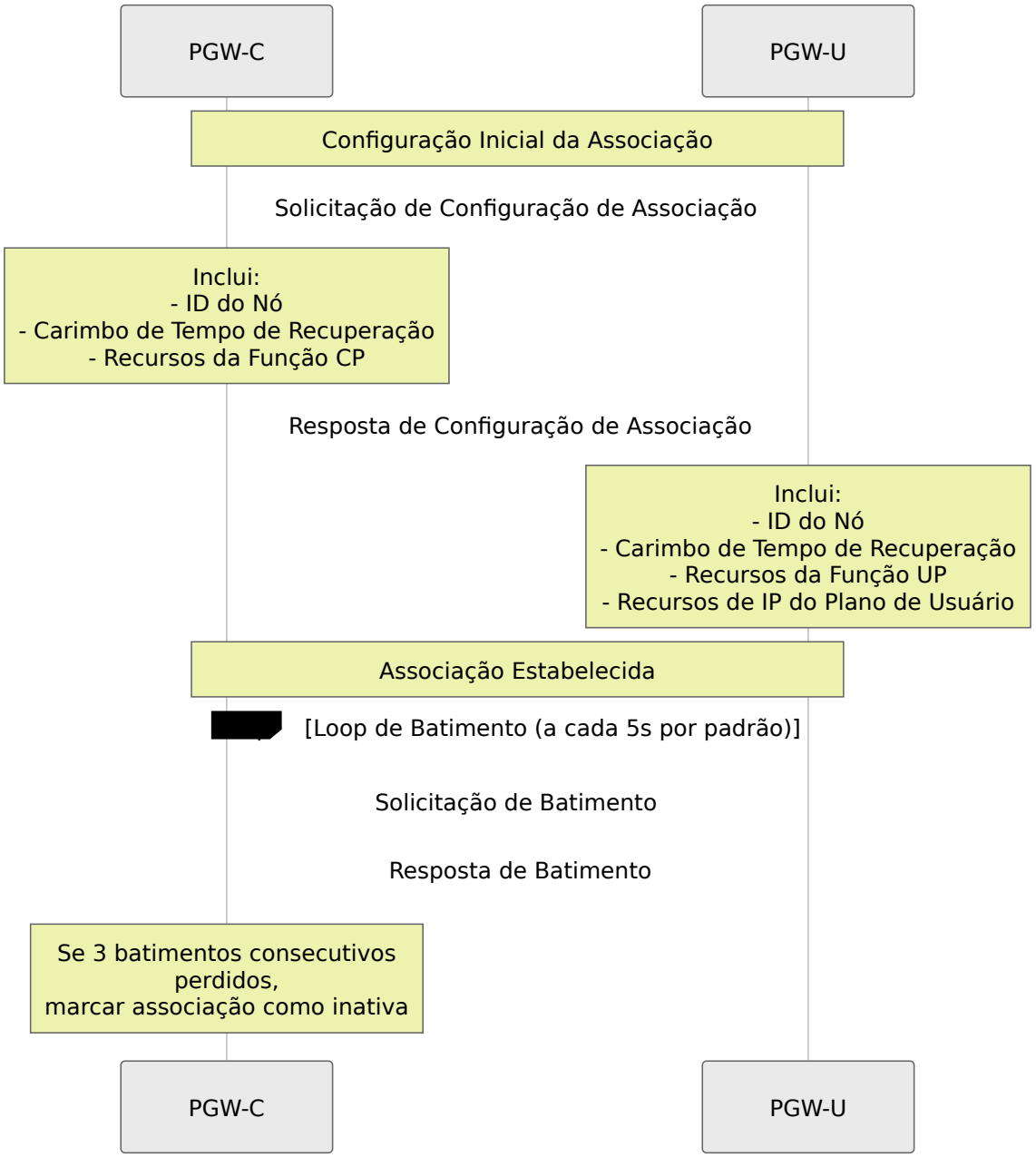
- **Endereço IPv4** - Mais comum

- **Endereço IPv6**
- **FQDN** (Nome de Domínio Totalmente Qualificado)

Gerenciamento de Associaç��o PFCP

Antes que o gerenciamento de sessão possa ocorrer, uma **associação** PFCP deve ser estabelecida entre o PGW-C e o PGW-U.

Fluxo de Configuração de Associação



Gerenciamento de Estado do Par

Cada par PFCP mantém estado:

Campo	Descrição
`is_associated`	Booleano indicando o status da associação
`remote_node_id`	ID do Nó do par (IP ou FQDN)
`remote_ip_address`	Endereço IP para comunicação
`remote_port`	Porta UDP (padrão 8805)
`heartbeat_period_ms`	Intervalo de batimento em milissegundos
`missed_heartbeats_consecutive`	Contagem de batimentos perdidos
`up_function_features`	Recursos suportados do plano de usuário
`up_recovery_time_stamp`	Carimbo de tempo de recuperação do par

Mecanismo de Batimento

Objetivo: Detectar falhas de pares e manter a vivacidade da associação

Configuração:

```
# Em config/runtime.exs
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  fallback_pool: [
    %{remote_ip_address: "10.0.0.21", remote_port: 8805, weight:
100}
  ]
}
# Todos os UPFs são registrados automaticamente com batimentos de
5 segundos
```

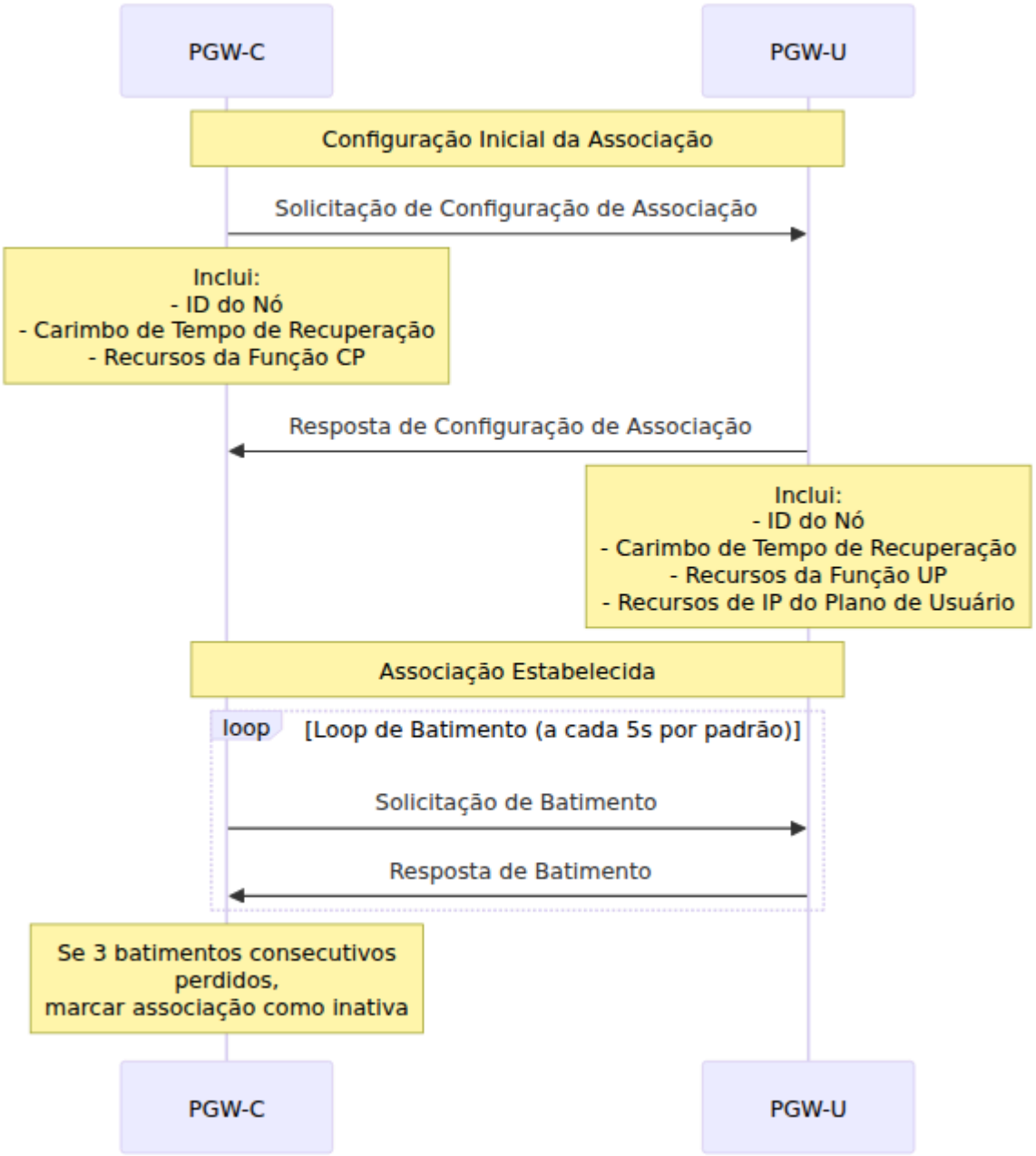
Detecção de Falhas:

- Cada batimento perdido incrementa `missed_heartbeats_consecutive`
- Geralmente configurado para falhar após 3 perdas consecutivas
- Associação falhada impede novas sessões para aquele par

Gerenciamento de Sessão PFCP

As sessões PFCP são criadas para cada conexão PDN de UE para programar regras de encaminhamento no plano de usuário.

Ciclo de Vida da Sessão



Estabelecimento de Sessão

Quando: UE se conecta e cria uma conexão PDN

PGW-C envia para PGW-U:

Solicitação de Estabelecimento de Sessão contendo:

- **SEID** (ID do Ponto de Extremidade da Sessão) - Identificador de sessão único

- **ID do Nó** - ID do Nó do PGW-C
- **F-SEID** - SEID Totalmente Qualificado (inclui IP + SEID)
- **PDRs** - Regras de Detecção de Pacotes (tipicamente 2: uplink + downlink)
- **FARs** - Regras de Ação de Encaminhamento (tipicamente 2: uplink + downlink)
- **QERs** - Regras de Aplicação de QoS (limites de bitrate)
- **BAR** - Regra de Ação de Buffering (para buffering de downlink)

PGW-U responde:

Resposta de Estabelecimento de Sessão contendo:

- **Causa** - Razão de sucesso ou falha
- **F-SEID** - Ponto de extremidade da sessão do PGW-U
- **PDRs Criados** - Confirmação das regras criadas
- **F-TEID** - TEID Totalmente Qualificado para a interface S5/S8

Modificação de Sessão

Quando: Mudanças de QoS, atualizações de pol��tica ou modificações de bearer ocorrem

A modificação pode incluir:

- Adicionar novos PDRs, FARs, QERs
- Remover regras existentes
- Atualizar parâmetros de regra

Exclusão de Sessão

Quando: UE se desconecta ou a conexão PDN é encerrada

Processo:

1. PGW-C envia Solicitação de Exclusão de Sessão com SEID
2. PGW-U remove todas as regras e libera recursos
3. PGW-U responde com Resposta de Exclusão de Sessão

Alocação de F-TEID

F-TEID (Identificador de Ponto de Extremidade de Túnel Totalmente Qualificado) identifica pontos de extremidade de túnel GTP-U para tráfego do plano de usuário. Ao estabelecer uma sessão PFCP, alguém deve alocar o F-TEID que identifica onde o UPF deve enviar tráfego de uplink. Existem duas abordagens:

Entendendo a Alocação de F-TEID

O que está sendo alocado: O F-TEID consiste em:

- **TEID** (Identificador de Ponto de Extremidade de Túnel) - Número de 32 bits identificando o túnel
- **Endereço IP** - Para onde enviar pacotes GTP-U (o endereço IP do UPF)

A Pergunta: Quem aloca o valor TEID?

Opção 1: UPF Aloca (Padrão Recomendado)

- PGW-C diz "por favor, aloque um TEID para mim" (flag CHOOSE)
- UPF escolhe um TEID de seu pool local e responde com o valor

Opção 2: PGW-C Aloca (Modo de Compatibilidade)

- PGW-C escolhe um TEID e diz ao UPF "use este TEID específico"
- UPF usa o TEID fornecido sem alocação

Alocação UPF (Padrão - Recomendado)

Configuração:

```
sxb: %{
  allocate_uplink_f_teid: false  # Padrão
}
```

Como Funciona:

1. PGW-C constrói a Solicitação de Estabelecimento de Sessão PFCP com a flag CHOOSE do F-TEID
2. UPF recebe a solicitação, aloca TEID de seu pool interno
3. UPF responde com o F-TEID alocado (TEID + endereço IP)
4. PGW-C armazena o F-TEID alocado durante a vida útil da sessão

Por que isso é melhor (geralmente):

□ Separação de Preocupações

- UPF possui o plano de usuário = UPF gerencia identificadores do plano de usuário
- Não há necessidade de PGW-C rastrear quais TEIDs o UPF tem disponíveis
- Cada componente gerencia seu próprio pool de recursos

□ Escalabilidade Multi-PGW-C

- Múltiplas instâncias de PGW-C podem se comunicar com o mesmo UPF sem coordenação
- Sem risco de colisões de TEID entre diferentes instâncias de PGW-C
- UPF garante unicidade entre todos os pares do plano de controle

□ Comportamento Padrão 3GPP

- A flag CHOOSE é definida na 3GPP TS 29.244 para esse propósito
- Implementações modernas de UPF a suportam
- Segue o princípio "deixe o proprietário alocar"

□ Failover Mais Simples

- Se o PGW-C reiniciar, o UPF ainda possui o namespace de TEID
- Não há necessidade de sincronizar o estado de alocação de TEID
- UPF pode continuar usando TEIDs existentes

Quando Usar:

- □ Implantações de produção com UPFs modernos (padrão)
- □ Implantações Multi-PGW-C compartilhando pools de UPF

- □ Arquiteturas nativas da nuvem com planos de controle sem estado
- □ Você quer comportamento padrão 3GPP PFCP

Problemas Potenciais:

- ⚠ Algumas implementações de UPF legadas ou proprietárias não suportam a flag CHOOSE
- ⚠ Se o estabelecimento da sessão falhar com "IE obrigatória ausente" ou similar, o UPF pode não suportar CHOOSE

Alocação PGW-C (Compatibilidade Legada)

Configuração:

```
sxb: %{
  allocate_uplink_f_teid: true
}
```

Como Funciona:

1. PGW-C aloca TEID de seu pool local durante a criação da sessão
2. PGW-C constrói a Solicitação de Estabelecimento de Sessão PFCP com um valor TEID explícito
3. UPF recebe a solicitação, usa o TEID fornecido sem alocação
4. Tanto PGW-C quanto UPF rastreiam o mesmo valor TEID

Por que você pode precisar disso:

□ UPF Não Suporta CHOOSE

- Algumas implementações de UPF (especialmente legadas/proprietárias) não suportam alocação dinâmica
- UPF espera um TEID explícito na Solicitação de Estabelecimento de Sessão PFCP
- Única solução para compatibilidade

□ Gerenciamento Centralizado de TEID

- Se você precisa que o PGW-C tenha total visibilidade sobre todos os TEIDs alocados
- Útil para depuração de problemas do plano de usuário (PGW-C conhece os valores exatos de TEID)
- Pode correlacionar TEID em capturas de pacotes com o estado da sessão

□ Alocação Determinística

- Se você precisa de padrões de alocação de TEID previsíveis
- Alguns ambientes de teste podem exigir faixas específicas de TEID

Compensações:

⚠ Coordenação Necessária para Multi-PGW-C

- Múltiplas instâncias de PGW-C compartilhando um UPF devem evitar colisões de TEID
- Requer:
  - Faixas de TEID particionadas por PGW-C (configuração complexa)
  - Serviço de alocação de TEID compartilhado (infraestrutura adicional)
  - Aceitar risco de colisão com alocação aleatória (baixa probabilidade)

⚠ Sincronização de Estado

- PGW-C deve rastrear TEIDs alocados para evitar reutilização
- Estado do pool de TEID perdido na reinicialização do PGW-C (deve ser reconstruído a partir das sessões)
- Cenários de failover mais complexos

⚠ Comportamento Não Padrão

- Não é o padrão de design PFCP pretendido
- Pode não funcionar com todas as implementações de UPF que esperam CHOOSE

Quando Usar:

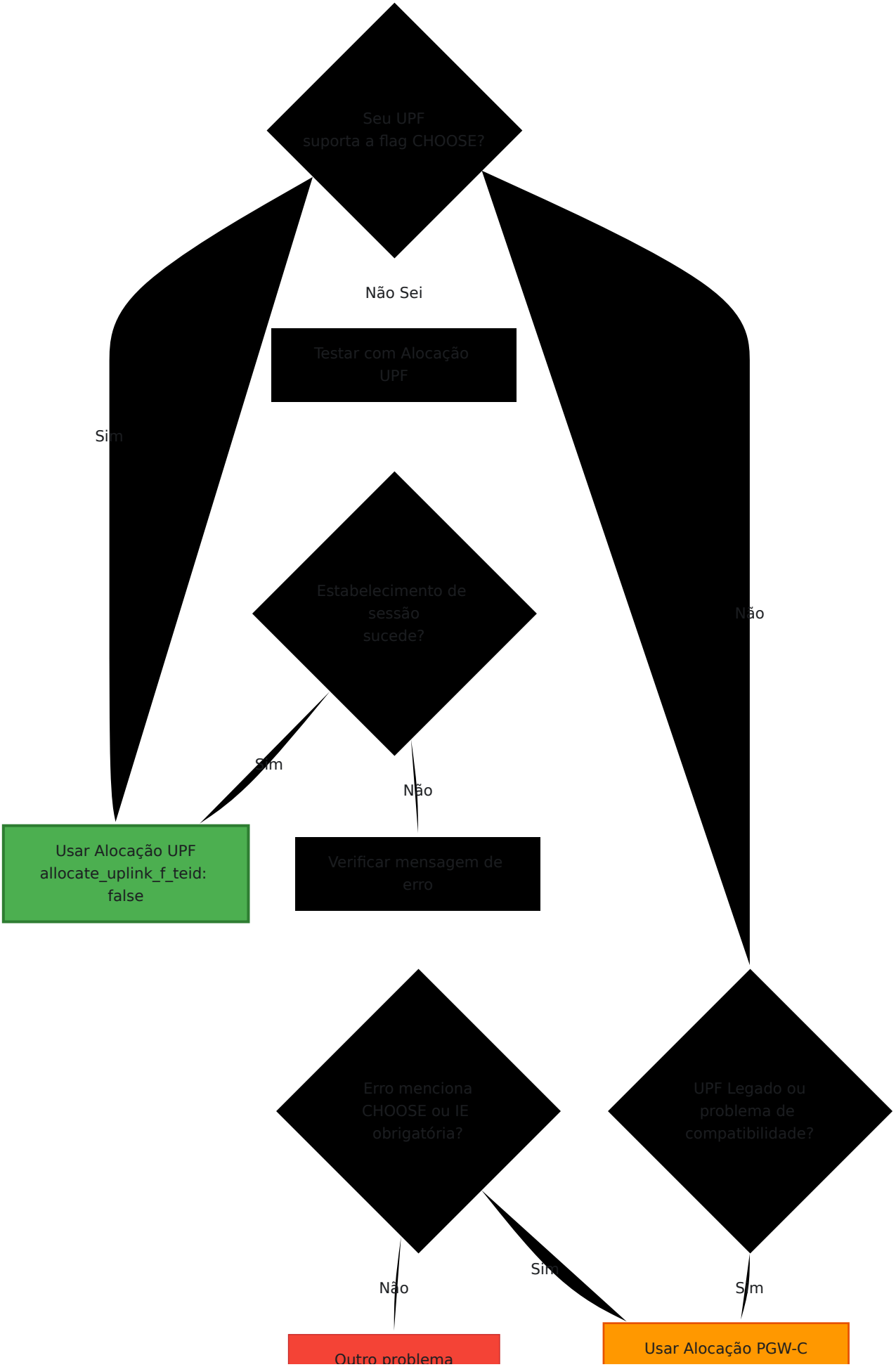
- **⚠ Apenas quando o UPF não suportar a flag CHOOSE**

- ⚠ Implementações legadas de UPF (por exemplo, algum hardware proprietário)
- ⚠ Requisitos específicos de compatibilidade
- ⚠ Cenários de depuração que exigem visibilidade de TEID do PGW-C

Tratamento de Colisão de TEID: O PGW-C usa alocação aleatória com detecção de colisão:

- Faixa de TEID: 1 a 0xFFFFFFFF (4,2 bilhões de valores)
- Probabilidade de colisão: ~0,023% a 1 milhão de sessões
- Tentativa automática em caso de colisão (transparente para o chamador)
- TEIDs liberados automaticamente quando a sessão termina

Como Escolher


Seu UPF suporta a flag CHOOSE?
Não Sei
Testar com Alocação UPF
Sim
Não
Estabelecimento de sessão sucede?
Sim
Não
Usar Alocação UPF allocate_uplink_f_teid: false
Verificar mensagem de erro
Erro menciona CHOOSE ou IE obrigatória?
UPF Legado ou problema de compatibilidade?
Não
Sim
Sim
Outro problema
Usar Alocação PGW-C

Solução de Problemas

Sintoma: Estabelecimento de sessão falha imediatamente

Verifique os logs PFCP:

```
# Procure por erros relacionados a CHOOSE
grep -i "choose\|mandatory.*missing" /var/log/pgw_c.log

# Verifique os códigos de causa da Resposta de Estabelecimento de
Sessão PFCP
grep "Session Establishment Response" /var/log/pgw_c.log
```

Se o UPF rejeitar a flag CHOOSE:

- O erro pode dizer "IE obrigatória ausente" ou "IE inválida"
- O UPF espera um F-TEID explícito, mas recebeu CHOOSE
- **Solução:** Defina `allocate_uplink_f_teid: true`

Se a alocação PGW-C causar problemas:

- Muito raro - o espaço de TEID é enorme (4 bilhões de valores)
- Verifique a exaustão de TEID (improvável abaixo de milhões de sessões):

```
# Verifique a contagem do registro
grep "registered_teid_count" /var/log/pgw_c.log
```

Alternando Entre Modos:

```
# Edite config/runtime.exs
sxb: %{
  local_ip_address: "10.0.0.20",
  allocate_uplink_f_teid: false  # Mude para true se o UPF não
suportar CHOOSE
}
```

Em seguida, reinicie o PGW-C:

```
systemctl restart pgw_c
```

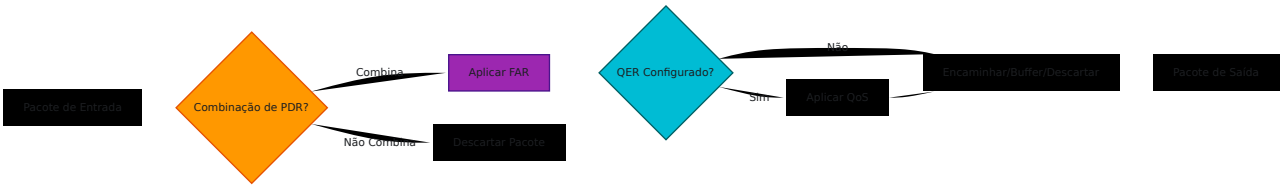
Verificando Qual Modo Está Ativo: Verifique as capturas de pacotes PFCP:

```
# Capture o tráfego PFCP
tcpdump -i any -n port 8805 -w pfcp.pcap

# Abra no Wireshark e veja a Solicitação de Estabelecimento de
Sessão
# Se o F-TEID mostrar "CHOOSE" flags: modo de alocação UPF
# Se o F-TEID mostrar valor TEID explícito: modo de alocação PGW-C
```

Regras de Processamento de Pacotes

O PFCP usa um conjunto de regras para definir como o plano de usuário processa pacotes.

Arquitetura da Regra



PDR (Regra de Detecção de Pacote)

Objetivo: Identificar quais pacotes esta regra se aplica

Configuração Típica do PGW-C:

PDR #1 - Downlink:

```
ID do PDR: 1
Precedência: 100
PDI (Informação de Detecção de Pacote):
  - Interface de Origem: CORE (lado da Internet)
  - Endereço IP do UE: 100.64.1.42/32
ID do FAR: 1 (regra de encaminhamento associada)
```

PDR #2 - Uplink:

```
ID do PDR: 2
Precedência: 100
PDI (Informação de Detecção de Pacote):
  - Interface de Origem: ACCESS (lado do SGW)
  - F-TEID: <ponto de extremidade do túnel S5/S8>
ID do FAR: 2 (regra de encaminhamento associada)
ID do QER: 1 (aplicação de QoS)
```

Campos Chave do PDR:

- **ID do PDR** - Identificador único da regra (por sessão)
- **Precedência** - Prioridade de correspondência da regra (mais alto = mais específico)
- **PDI** - Critérios de correspondência (interface, IP, TEID, etc.)
- **Remoção do Cabeçalho Externo** - Remover cabeçalho GTP-U na entrada
- **ID do FAR** - Ação de encaminhamento associada
- **ID do QER** - Aplicação de QoS associada (opcional)

FAR (Regra de Ação de Encaminhamento)

Objetivo: Definir o que fazer com pacotes combinados

FAR #1 - Downlink (Internet → UE):

```
ID do FAR: 1
Aplicar Ação: ENCAMINHAR
Parâmetros de Encaminhamento:
  - Interface de Destino: ACCESS (para SGW)
  - Criação de Cabeçalho Externo: GTP-U/UDP/IPv4
  - F-TEID Remoto: <ponto de extremidade do túnel SGW S5/S8>
```

FAR #2 - Uplink (UE → Internet):

```
ID do FAR: 2
Aplicar Ação: ENCAMINHAR
Parâmetros de Encaminhamento:
  - Interface de Destino: CORE (para Internet)
  - (Sem cabeçalho externo - encaminhamento IP simples)
```

Campos Chave do FAR:

- **ID do FAR** - Identificador único da regra
- **Aplicar Ação** - ENCAMINHAR, DESCARTAR, BUFFER, NOTIFICAR
- **Parâmetros de Encaminhamento:**
  - Interface de destino (ACCESS/CORE)
  - Criação de Cabeçalho Externo (adicionar túnel GTP-U)
  - Instância de Rede (VRF/tabela de roteamento)

QER (Regra de Aplicação de QoS)

Objetivo: Aplicar limites de bitrate e parâmetros de QoS. Os QERs também podem rastrear uso para gerenciamento de cotas de cobrança online (veja Interface Diameter Gy para controle de crédito).

Exemplo de QER:

```
ID do QER: 1
Status do Portão: ABERTO
Bitrate Máximo:
  - Uplink: 100 Mbps
  - Downlink: 50 Mbps
Bitrate Garantido: (opcional, para bearers GBR)
  - Uplink: 10 Mbps
  - Downlink: 10 Mbps
```

Campos Chave do QER:

- **ID do QER** - Identificador único da regra
- **Status do Portão** - ABERTO (permitir) ou FECHADO (bloquear)
- **MBR** - Bitrate Máximo (uplink/downlink)
- **GBR** - Bitrate Garantido (para bearers dedicados)
- **QCI** - Identificador de Classe de QoS (afeta o agendamento)

BAR (Regra de Ação de Buffering)

Objetivo: Controlar o buffering de pacotes de downlink quando o UE está ocioso

Exemplo de BAR:

```
ID do BAR: 1
Atraso de Notificação de Dados de Downlink: 100ms
Contagem Sugerida de Pacotes a Serem Bufferizados: 10
```

Usado para: Otimização de DRX (Recepção Descontínua) em modo ocioso

---

Configuração

Configuração Básica do Sxb

Edite `config/runtime.exs`:

```
config :pgw_c,
  sxb: %{
    # Endereço IP local para comunicação PFCP
    local_ip_address: "10.0.0.20",

    # Opcional: Substituir a porta padrão (8805)
    local_port: 8805,

    # Tempo limite de solicitação PFCP em milissegundos (padrão:
500ms)
    # Tempo a esperar pela resposta do UPF antes de retransmitir
    # Deve ser >= tempo de processamento esperado do UPF para
evitar sessões duplicadas
    request_timeout_ms: 500,

    # Número de tentativas de retransmissão para solicitações PFCP
(padrão: 3)
    # Tempo total máximo de espera = request_timeout_ms *
request_attempts
    request_attempts: 3,

    # Opcional: Controlar alocação de F-TEID para o plano de
usuário
    # Quando falso (padrão): UPF aloca F-TEID (flag CHOOSE)
    # Quando verdadeiro: PGW-C pré-aloca F-TEID e fornece valor
explícito
    # Nota: Alguns UPFs podem não suportar a flag CHOOSE e exigir
alocação explícita
    allocate_uplink_f_teid: false
  },

  # Seleção de UPF - Todos os UPFs definidos aqui são registrados
automaticamente
  upf_selection: %{
    fallback_pool: [
      %{
        # Endereço IP do PGW-U
        remote_ip_address: "10.0.0.21",

        # Porta PFCP (padrão: 8805)
        remote_port: 8805,

        # Peso para balanceamento de carga (100 = normal, 0 =
```

```
reserva)
        weight: 100
      }
    ]
  }
```

Configuração de Tempo Limite de Solicitação

A interface PFCP usa tempos limites configuráveis para Solicitações de Estabelecimento, Modificação e Exclusão de Sessão para o UPF.

Parâmetros:

Parâmetro	Tipo	Padrão	Descrição
`request_timeout_ms`	Inteiro	500	Tempo em milissegundos para esperar pela resposta do UPF antes de retransmitir
`request_attempts`	Inteiro	3	Número máximo de tentativas de transmissão antes de falhar a solicitação

Tempo Total de Espera: `request_timeout_ms × request_attempts`

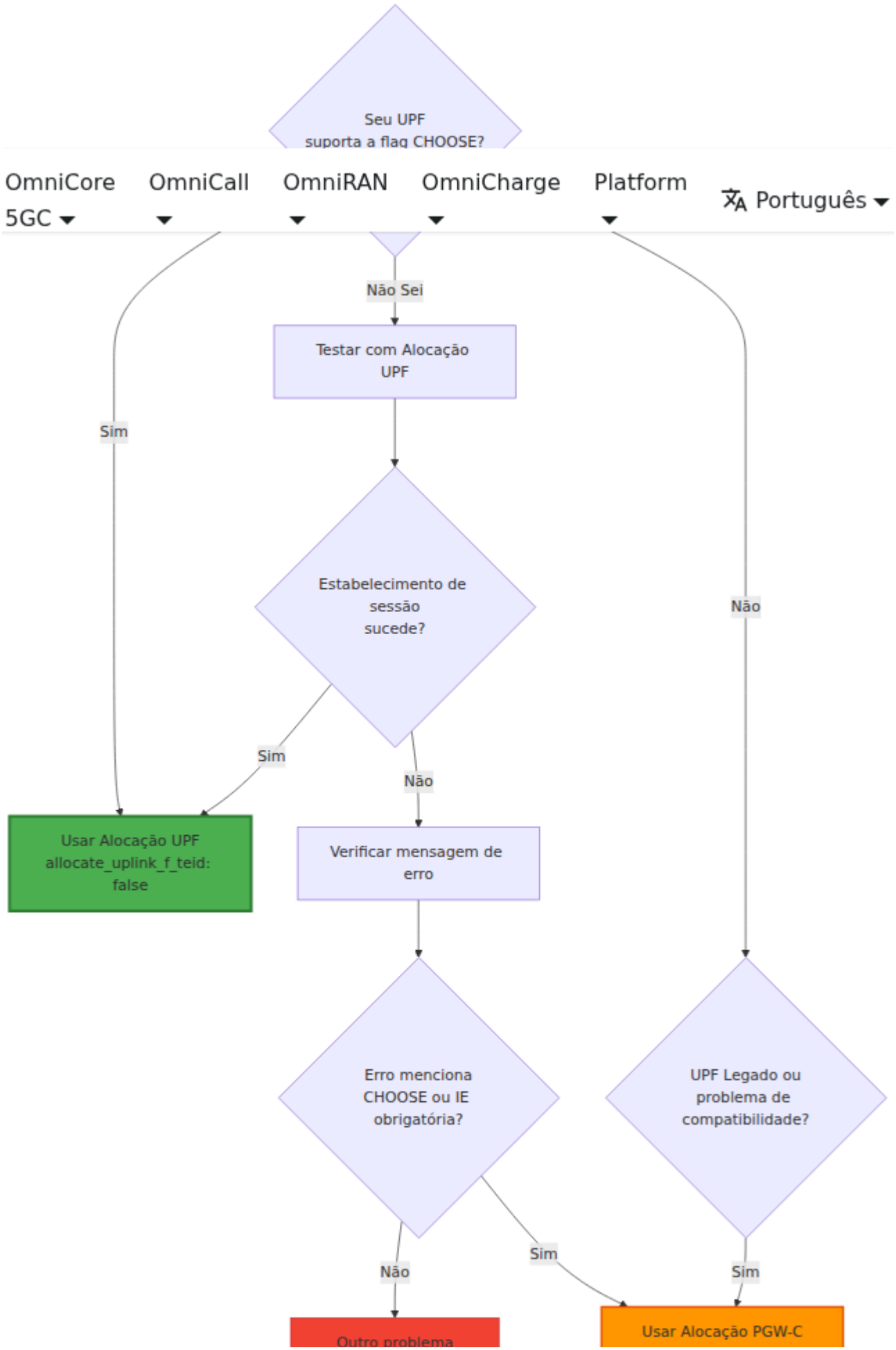
Comportamento padrão: 500ms × 3 tentativas = **1,5 segundos de espera máxima total**

Por que a Configuração de Tempo Limite é Importante

Se `request_timeout_ms` estiver definido muito baixo em relação ao tempo de processamento do UPF:

1. PGW-C envia Solicitação de Estabelecimento de Sessão
2. O tempo limite expira antes que o UPF responda
3. PGW-C retransmite com o mesmo número de sequência
4. O UPF processa ambas as solicitações e cria **sessões PFCP duplicadas**
5. PGW-C recebe a primeira resposta e armazena um ID de sessão

6. A segunda sessão se torna **órfã** no UPF


Seu UPF suporta a flag CHOOSE?
OmniCore 5GC
OmniCall
OmniRAN
OmniCharge
Platform
Português
Não Sei
Testar com Alocação UPF
Sim
Estabelecimento de sessão sucede?
Não
Sim
Usar Alocação UPF allocate_uplink_f_teid: false
Verificar mensagem de erro
Erro menciona CHOOSE ou IE obrigatória?
Não
Sim
Outro problema
UPF Legado ou problema de compatibilidade?
Sim
Usar Alocação PGW-C

Diretrizes de Ajuste

Tempo de Resposta do UPF	`request_timeout_ms` Recomendado	Tempo Total de Espera
Rápido (<100ms)	200-300ms	600-900ms (3 tentativas)
Normal (100-300ms)	500ms (padrão)	1,5s (3 tentativas)
Lento (300-500ms)	750-1000ms	2,25-3s (3 tentativas)
Muito lento (>500ms)	1500-2000ms	4,5-6s (3 tentativas)

Recomendação: Defina `request_timeout_ms` para pelo menos **2× o tempo de resposta esperado do UPF** para evitar sessões órfãs induzidas por retransmissão.

Exemplo - UPF Lento

```
sxb: %{
  local_ip_address: "10.0.0.20",
  request_timeout_ms: 1000,  # 1 segundo por tentativa
  request_attempts: 3         # Total: 3 segundos no máximo
}
```

Diagnóstico de Problemas de Tempo Limite

Sintomas de tempo limite muito baixo:

- O UPF relata mais sessões PFCP do que o esperado
- Sessões órfãs se acumulam no UPF ao longo do tempo
- Mensagens de log: `"Solicitação de Estabelecimento de Sessão expirou"` seguidas por sessão bem-sucedida

Como diagnosticar:

1. Verifique a contagem de sessões do UPF via API ou interface de gerenciamento do UPF
2. Compare com a contagem de sessões ativas do PGW-C
3. Se o UPF tiver mais sessões, as órfãs existem devido a retransmissões

Resolução:

1. Aumente `request_timeout_ms` para exceder o tempo de resposta do UPF
2. Reinicie o PGW-C para aplicar a nova configuração
3. Limpe as sessões órfãs do UPF (limpeza manual ou reinicialização do UPF)

Múltiplos Pares PGW-U

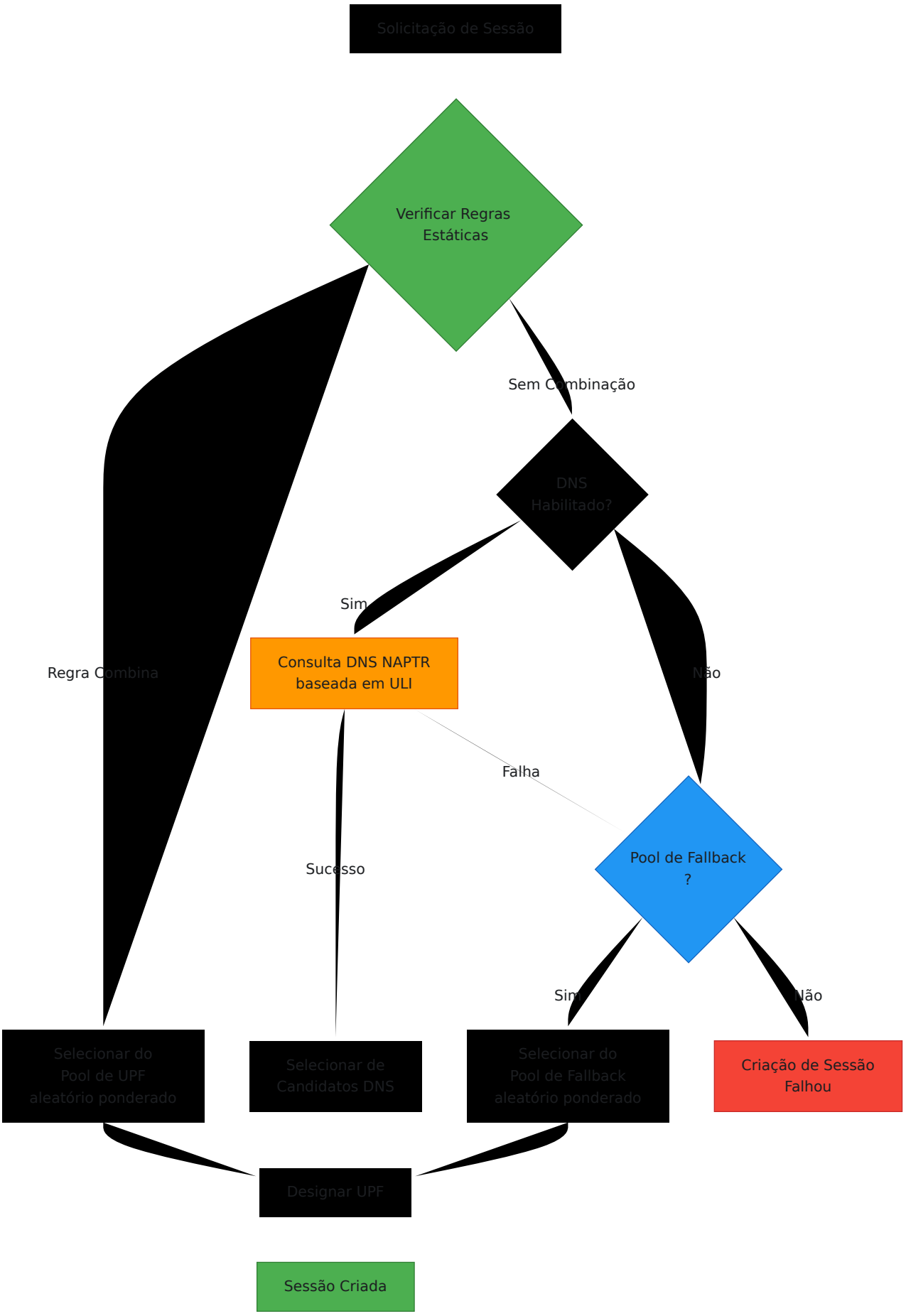
Para balanceamento de carga ou redundância:

```
config :pgw_c,
  sxb: %{
    local_ip_address: "10.0.0.20"
  },
  upf_selection: %{
    fallback_pool: [
      %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight:
50},  # 50% do tráfego
      %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight:
50}   # 50% do tráfego
    ]
  }
# Ambos os UPFs registrados automaticamente com batimentos de 5
segundos
```

Configuração de Seleção de UPF

O PGW-C usa um **sistema de seleção de UPF em três camadas** com regras baseadas em prioridade:

1. **Regras Estáticas** (Maior Prioridade) - Correspondem com base em atributos da sessão
2. **Seleção Baseada em DNS** (Prioridade Média) - Roteamento ciente da localização via consultas DNS NAPTR
3. **Pool de Fallback** (Menor Prioridade) - Pool de UPF padrão quando nenhuma regra corresponde


Solicitação de Sessão
Verificar Regras Estáticas
Regra Combina
Sem Combinação
DNS Habilitado?
Sim
Não
Consulta DNS NAPTR baseada em ULI
Falha
Sucesso
Pool de Fallback ?
Sim
Não
Selecionar do Pool de UPF aleatório ponderado
Selecionar de Candidatos DNS
Selecionar do Pool de Fallback aleatório ponderado
Criação de Sessão Falhou
Designar UPF
Sessão Criada

Exemplo Completo de Seleção de UPF

```
config :pgw_c,
  # Interface PFCP
  sxb: %{
    local_ip_address: "10.0.0.20"
  },

  # Seleção de UPF: Todos os UPFs definidos aqui são registrados
automaticamente
  upf_selection: %{
    #
=============================================================================
    # Seleção Baseada em DNS (Roteamento Ciente da Localização)
    #
=============================================================================
    # Consulta DNS usando Informação de Localização do Usuário (ULI)
    # Fornece seleção dinâmica de UPF com base na localização da
célula
    dns_enabled: false,
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
    dns_suffix: "epc.3gppnetwork.org",
    dns_timeout_ms: 5000,

    #
=============================================================================
    # Regras de Seleção Estáticas (Avaliada por Prioridade)
    #
=============================================================================
    # As regras são verificadas da maior para a menor prioridade
    # A primeira regra correspondente determina o pool de UPF
    rules: [
      # Regra 1: Tráfego IMS - Maior Prioridade
      %{
        name: "Tráfego IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [
          %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
          %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
        ],
        # Opcional: Sobrescritas de PCO para esta regra
```

```
        pco: %{
          p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
        }
      },

      # Regra 2: APN Empresarial - Alta Prioridade
      %{
        name: "Tráfego Empresarial",
        priority: 15,
        match_field: :apn,
        match_regex: "^(enterprise|corporate)\.apn",
        upf_pool: [
          %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
        ],
        pco: %{
          primary_dns_server_address: "192.168.1.10",
          secondary_dns_server_address: "192.168.1.11",
          ipv4_link_mtu_size: 1500
        }
      },

      # Regra 3: Assinantes em Roaming - Prioridade Média
      %{
        name: "Assinantes em Roaming",
        priority: 10,
        match_field: :serving_network_plmn_id,
        match_regex: "^(310|311|312|313)",  # Redes dos EUA
        upf_pool: [
          %{remote_ip_address: "10.100.4.21", remote_port: 8805,
weight: 100}
        ]
      },

      # Regra 4: Tráfego da Internet - Menor Prioridade
      %{
        name: "Tráfego da Internet",
        priority: 5,
        match_field: :apn,
        match_regex: "^internet",
        upf_pool: [
          %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 33},
          %{remote_ip_address: "10.100.1.22", remote_port: 8805,
```

```
weight: 33},
          %{remote_ip_address: "10.100.1.23", remote_port: 8805,
weight: 34}
        ]
      }
    ],

    #
=================================================================
    # Pool de Fallback (Último Recurso)
    #
=================================================================
    # Usado quando nenhuma regra corresponde e a seleção DNS falha ou
está desabilitada
    fallback_pool: [
      %{remote_ip_address: "127.0.0.21", remote_port: 8805, weight:
100}
    ]
  }
```

Campos de Correspondência Suportados

Campo de Correspondência	Descrição	Valor de Exemplo
`:imsi`	Identidade Internacional de Assinante Móvel	`"310260123456789"`
`:apn`	Nome do Ponto de Acesso	`"internet"`, `"ims"`
`:serving_network_plmn_id`	PLMN da rede de serviço (MCC+MNC)	`"310260"` (operadora dos EUA)
`:sgw_ip_address`	Endereço IP do SGW (formato de string)	`"10.0.1.50"`
`:uli_tai_plmn_id`	ID de PLMN da Área de Rastreamento	`"310260"`
`:uli_ecgi_plmn_id`	ID Global da Célula E-UTRAN	`"310260"`

Pool de UPF e Balanceamento de Carga

Cada regra pode especificar um **pool de UPF** com seleção aleatória ponderada:

```
upf_pool: [
  %{remote_ip_address: "10.100.1.21", remote_port: 8805, weight:
50},
  %{remote_ip_address: "10.100.1.22", remote_port: 8805, weight:
30},
  %{remote_ip_address: "10.100.1.23", remote_port: 8805, weight:
20}
]
```

Como Funciona a Seleção Ponderada:

1. Calcule o peso total: 50 + 30 + 20 = 100
2. Gere um número aleatório: 0.0 a 100.0
3. Selecione o UPF com base nas faixas de peso cumulativo:
    - 0-50: UPF-1 (50% de chance)
    - 50-80: UPF-2 (30% de chance)
    - 80-100: UPF-3 (20% de chance)

Casos de Uso:

- **Distribuição igual:** Todos os pesos iguais (33, 33, 34)
- **Primário/reserva:** Primário de alto peso (80), reserva de baixo peso (20)
- **Baseado em capacidade:** Peso proporcional à capacidade do UPF

Sobrescritas de PCO

As regras podem sobrescrever valores de PCO (Opções de Configuração de Protocolo):

```
%{
  name: "Tráfego IMS",
  match_field: :apn,
  match_regex: "^ims",
  upf_pool: [...],
  pco: %{
    # Sobrescrever apenas campos específicos
    p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"],
    # Outros campos usam valores padrão da configuração principal
de pco
  }
}
```

Campos de Sobrescrita de PCO Disponíveis:

- `primary_dns_server_address`
- `secondary_dns_server_address`
- `primary_nbns_server_address`

- `secondary_nbns_server_address`
- `p_cscf_ipv4_address_list`
- `ipv4_link_mtu_size`

Seleção Baseada em DNS

Quando habilitada, o PGW-C realiza consultas DNS NAPTR com base na Informação de Localização do Usuário:

```
upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
  dns_suffix: "epc.3gppnetwork.org",
  dns_timeout_ms: 5000
}
```

Prioridade da Consulta:

1. **ECGI** (Identificador Global da Célula E-UTRAN) - Mais específico
2. **TAI** (Identidade da Área de Rastreamento) - Área da célula
3. **RAI** (Identidade da Área de Roteamento) - Área 3G/2G
4. **SAI** (Identidade da Área de Serviço) - Área de serviço 3G
5. **CGI** (Identidade Global da Célula) - Célula 2G

Exemplo de Consulta DNS:

```
# Para consulta ECGI:
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org

# Para consulta TAI:
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Processo de Seleção DNS:

1. Tente consultas na ordem de prioridade (ECGI primeiro, depois TAI, etc.)
2. Se o DNS retornar candidatos, use o primeiro resultado (registrado dinamicamente se necessário)

3. Selecione o UPF retornado
4. Se nenhuma correspondência DNS ou DNS desabilitado, passe para o pool de fallback

Veja Seleção de UPF Baseada em DNS para informações detalhadas.

Seleção de UPF Baseada em DNS

Visão Geral

A seleção de UPF baseada em DNS fornece **roteamento ciente da localização** realizando consultas DNS NAPTR usando a Informação de Localização do Usuário (ULI) da célula atual do UE.

Referência 3GPP: TS 23.003 - Procedimentos DNS para descoberta de UPF

Benefícios:

- Seleção automática de UPF com base na localização geográfica
- Sem configuração manual de regras por célula
- Adaptação dinâmica a mudanças na topologia da rede
- Reduz o backhaul roteando para o UPF mais próximo

Como Funciona

Parse error on line 25: ... style PGWC fill:#4CAF50,stroke:#2E7 ----------
--^ Expecting 'SOLID_OPEN_ARROW', 'DOTTED_OPEN_ARROW',
'SOLID_ARROW', 'BIDIRECTIONAL_SOLID_ARROW', 'DOTTED_ARROW',
'BIDIRECTIONAL_DOTTED_ARROW', 'SOLID_CROSS', 'DOTTED_CROSS',
'SOLID_POINT', 'DOTTED_POINT', got 'TXT'

Tentar novamente

Configuração

```
config :pgw_c,
  upf_selection: %{
    # Habilitar seleção baseada em DNS
    dns_enabled: true,

    # Prioridade da consulta: tentar ECGI primeiro, depois TAI,
depois RAI, etc.
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],

    # Sufixo DNS para consultas
    dns_suffix: "epc.3gppnetwork.org",

    # Tempo limite da consulta DNS
    dns_timeout_ms: 5000,

    # Regras estáticas ainda têm precedência sobre DNS
    rules: [...],

    # Fallback se DNS falhar
    fallback_pool: [...]
  }
```

Formatos de Consulta DNS

As consultas DNS são construídas usando a Informação de Localização do Usuário (ULI) da mensagem GTP-C:

1. ECGI (Identificador Global da Célula E-UTRAN)

Mais específico - Roteamento em nível de célula LTE

Formato:

```
eci-<HEX-ECI>.ecgi.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemplo:

```
# ID da Célula: 0x1A2B3C (1.715.004 decimal)
# PLMN: MCC=999, MNC=999
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Quando Usado: Redes LTE (4G)

2. TAI (Identidade da Área de Rastreamento)

Área da célula - Múltiplas células na mesma área de rastreamento

Formato:

```
tac-lb<LB>.tac-hb<HB>.tac.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemplo:

```
# TAC: 0x0064 (100 decimal)
# Byte baixo: 0x64, Byte alto: 0x00
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Quando Usado: Áreas de rastreamento LTE (4G)

3. RAI (Identidade da Área de Roteamento)

Área de roteamento 3G/2G

Formato:

```
rac<RAC>.lac-lb<LB>.lac-hb<HB>.lac.rai.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Exemplo:

```
# RAC: 0x0A (10 decimal)
# LAC: 0x1234 (4660 decimal)
rac0a.lac-lb34.lac-hb12.lac.rai.mnc999.mcc999.epc.3gppnetwork.org
```

Quando Usado: Redes 3G/2G UMTS/GPRS

4. SAI (Identidade da Área de Serviço)

Área de serviço 3G

Formato:

```
sac<SAC>.lac-lb<LB>.lac-hb<HB>.lac.sai.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Exemplo:

```
# SAC: 0x0001
# LAC: 0x1234
sac0001.lac-lb34.lac-
hb12.lac.sai.mnc999.mcc999.epc.3gppnetwork.org
```

Quando Usado: Áreas de serviço 3G UMTS

5. CGI (Identidade Global da Célula)

Nível de célula 2G

Formato:

```
ci<CI>.lac-lb<LB>.lac-hb<HB>.lac.cgi.mnc<MNC>.mcc<MCC>.
<dns_suffix>
```

Exemplo:

```
# CI: 0x5678
# LAC: 0x1234
ci5678.lac-lb34.lac-hb12.lac.cgi.mnc999.mcc999.epc.3gppnetwork.org
```

Quando Usado: Células 2G GSM

Processamento da Resposta DNS

Formato do Registro NAPTR:

O DNS retorna registros NAPTR apontando para endereços IP de UPF:

```
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org.
  IN NAPTR 10 50 "a" "x-3gpp-upf:x-s5-gtp:x-s8-gtp" ""
upf1.epc.mnc999.mcc999.3gppnetwork.org.

upf1.epc.mnc999.mcc999.3gppnetwork.org.
  IN A 10.100.1.21
```

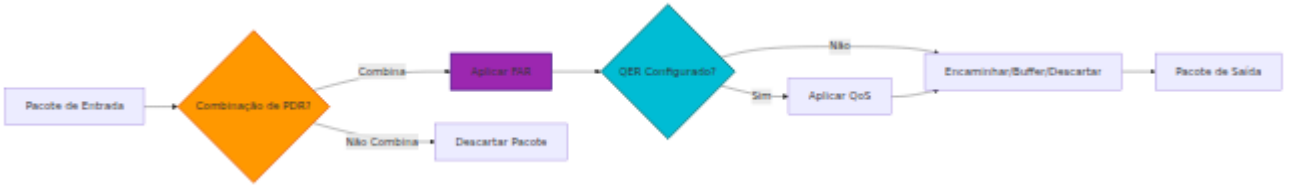
Processamento do PGW-C:

1. Analisa os registros NAPTR para extrair endereços IP de UPF
2. Seleciona o primeiro candidato da resposta DNS
3. Registra dinamicamente se ainda não estiver configurado (ou implementa seleção baseada em carga)

Exemplo:

```
DNS retorna: [10.100.1.21, 10.100.5.99, 10.100.3.50]

Selecionado:    10.100.1.21 (primeiro candidato)
Ação:          Registrar dinamicamente se não estiver na seleção
de upf
```

Exemplo de Prioridade de Seleção



Casos de Uso

1. Balanceamento de Carga Geográfica

Cenário: O operador tem UPFs em várias cidades

Configuração DNS:

```
# Célula de Chicago
eci-aaa.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-Chicago
(10.1.1.21)

# Célula de Nova York
eci-bbb.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-NewYork
(10.2.1.21)

# Célula de Los Angeles
eci-ccc.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-
LosAngeles (10.3.1.21)
```

Benefício: Usuários são automaticamente roteados para o UPF mais próximo, reduzindo latência e backhaul

2. Computação de Borda

Cenário: UPFs de MEC (Computação de Borda Multi-acesso) implantados em locais de célula

Configuração DNS:

```
# Cada célula aponta para o UPF de borda local
eci-*.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF de Borda
Local
```

Benefício: Latência ultra-baixa para aplicações de borda

3. Topologia de Rede Dinâmica

Cenário: Endereços de UPF mudam devido a atualizações ou manutenção

Benefício: Atualizar registros DNS sem mudar a configuração do PGW-C

Solução de Problemas de Seleção DNS

Falhas de Consulta DNS

Sintomas:

- Log: "Falha na seleção de UPF DNS: :nxdomain"
- Sessões caem no pool de fallback

Causas Possíveis:

1. Servidor DNS não configurado corretamente
2. Zona DNS não populada para IDs de célula
3. ULI não presente na mensagem GTP-C

Resolução:

```
# Testar consulta DNS manualmente
dig eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org NAPTR

# Verifique os logs do PGW-C para consultas DNS
grep "DNS UPF selection: querying" /var/log/pgw_c.log

# Verifique se ULI está presente na sessão
# Verifique o campo "uli" no estado da sessão
```

DNS Retorna UPF Desconhecido

Comportamento:

- DNS retorna um UPF candidato que não está na `upf_selection`
- O sistema tenta registrar dinamicamente
- Se a associação PFCP for bem-sucedida, o UPF é usado para a sessão
- Se a associação PFCP falhar, cai no pool de fallback

Exemplo:

```
DNS retorna: [10.99.1.50]
upf_selection: [10.100.1.21, 10.100.1.22]

Ação: Registrar dinamicamente 10.99.1.50
  - Enviar Configuração de Associação PFCP
  - Se sucesso: Usar para a sessão
  - Se tempo limite: Cair no pool de fallback
```

Opções de Resolução:

1. Pré-configurar em `upf_selection` para monitoramento imediato:

```
upf_selection: %{
  fallback_pool: [
    %{remote_ip_address: "10.99.1.50", remote_port: 8805, weight:
100}
  ]
}
```

2. Atualizar DNS para retornar endereços IP de UPF pré-configurados

3. Permitir registro dinâmico (recomendado para cenários de MEC/borda)

Tempo Limite de Consulta

Sintomas:

- Log: "Seleção de UPF DNS: tempo limite de consulta"
- Sessões demoram mais para serem estabelecidas

Resolução:

```
upf_selection: %{
  dns_timeout_ms: 10000  # Aumentar tempo limite para 10 segundos
}
```

Monitoramento da Seleção DNS

Métricas:

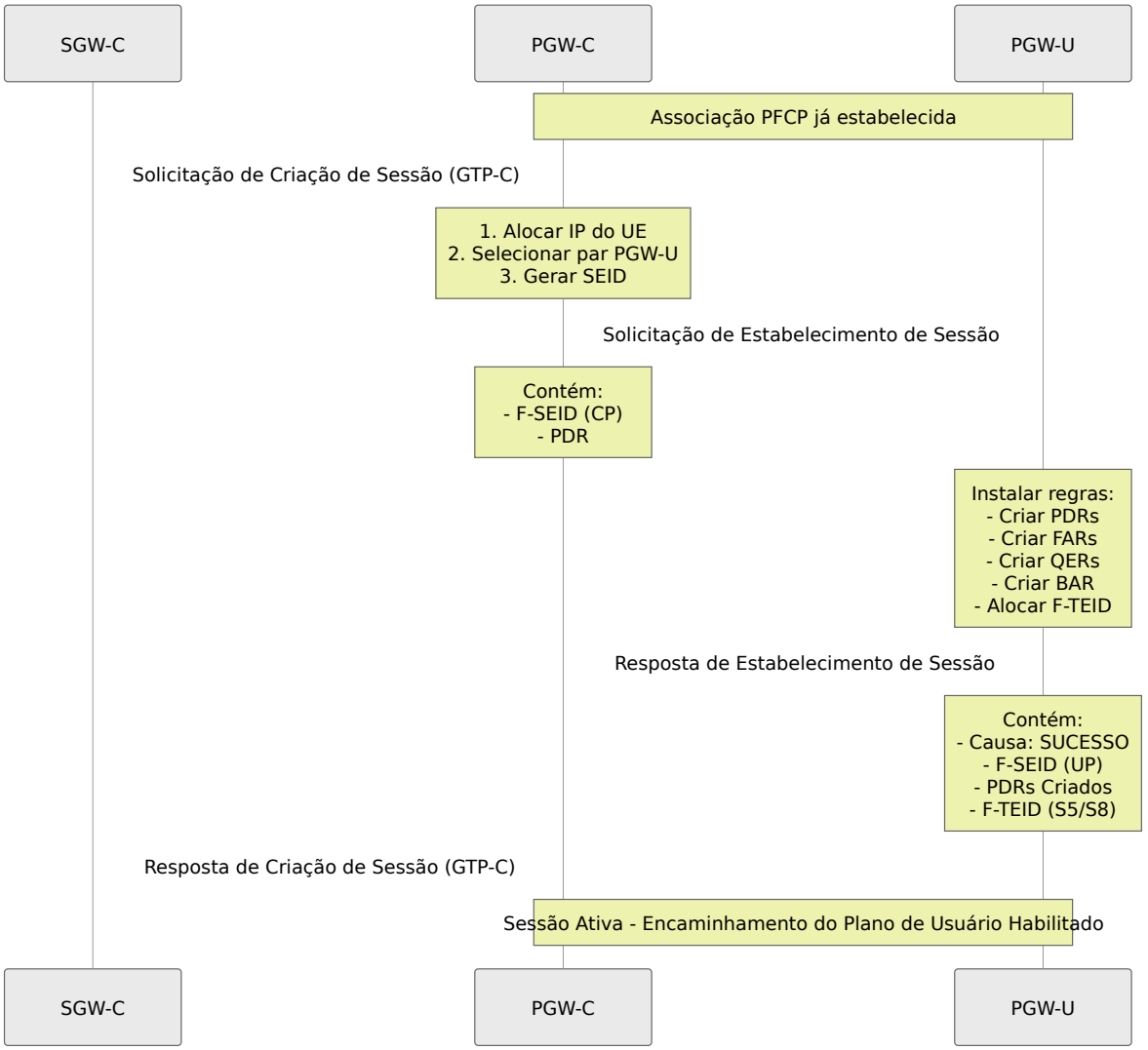
```
# Taxa de sucesso da consulta DNS
rate(upf_selection_dns_success_total[5m]) /
rate(upf_selection_dns_attempts_total[5m])

# Latência da consulta DNS
histogram_quantile(0.95,
rate(upf_selection_dns_duration_seconds_bucket[5m]))

# Uso de fallback (indica problemas de DNS)
rate(upf_selection_fallback_used_total[5m])
```

Exemplos de Logs:

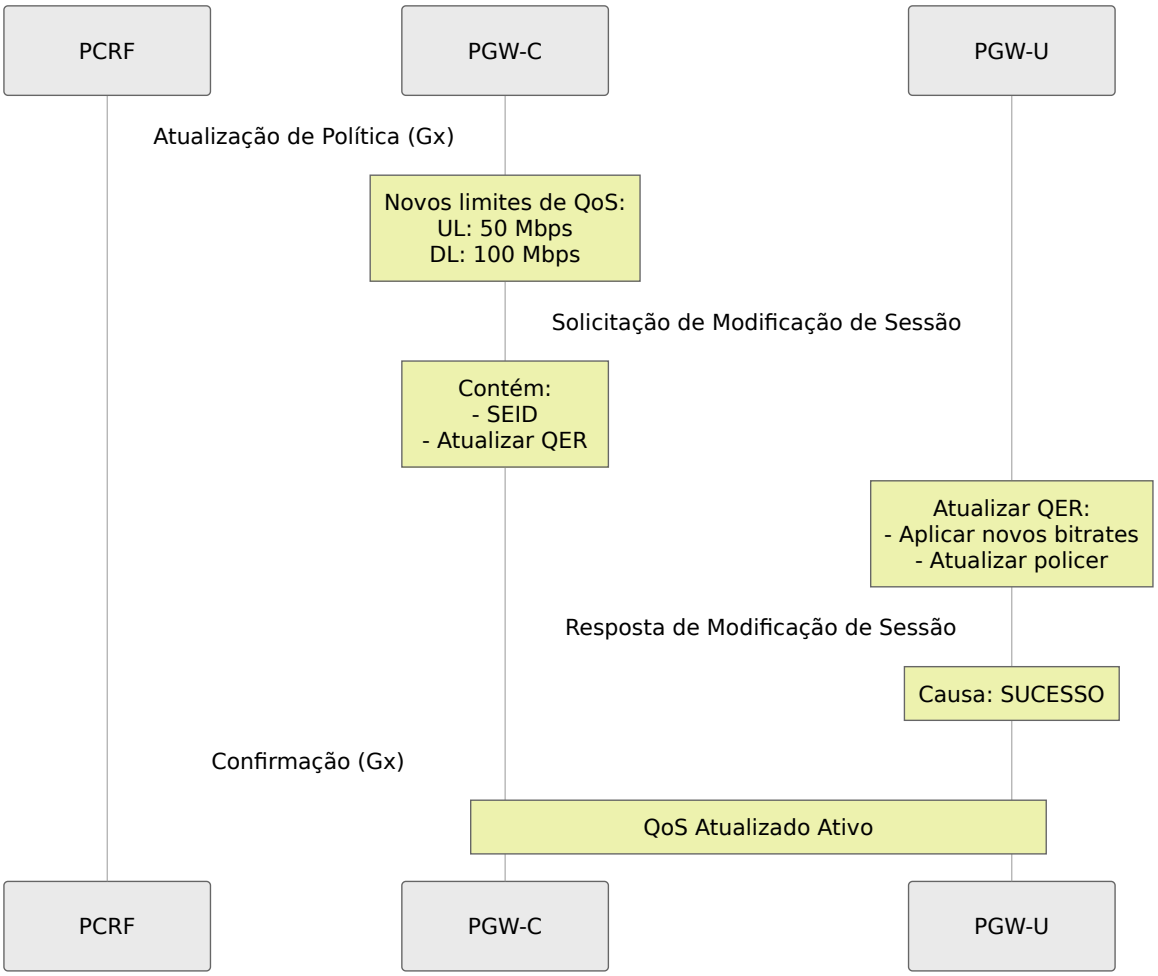
```
[debug] Seleção de UPF DNS: consultando eci-
1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
[debug] Seleção de UPF DNS: obteve 2 candidatos do DNS
[info]  Seleção de UPF DNS: selecionado 10.100.1.21
```

Fluxos de Mensagens

Fluxo Completo de Estabelecimento de Sessão



Fluxo de Modificação de Sessão



Recuperação de Falha de Batimento


Solicitação de Sessão
Verificar Regras Estáticas
Regra Combina
Sem Combinação
DNS Habilitado?
Sim
Não
Consulta DNS NAPTR baseada em ULI
Falha
Sucesso
Pool de Fallback ?
Sim
Não
Selecionar do Pool de UPF aleatório ponderado
Selecionar de Candidatos DNS
Selecionar do Pool de Fallback aleatório ponderado
Criação de Sessão Falhou
Designar UPF
Sessão Criada

Solução de Problemas

Problemas Comuns

1. Falha na Configuração da Associação

Sintomas:

- Mensagem de log: "Falha na Configuração da Associação PFCP"
- Sem resposta à Solicitação de Configuração de Associação

Causas Possíveis:

- PGW-U não acessível (problema de rede)
- PGW-U não está em execução
- Firewall bloqueando a porta UDP 8805
- ID de `remote_ip_address` incorreto na configuração

Resolução:

```
# Testar conectividade
ping <pgw_u_ip_address>

# Testar porta UDP
nc -u -v <pgw_u_ip_address> 8805

# Verificar firewall
iptables -L -n | grep 8805
```

2. Falhas de Batimentos

Sintomas:

- Log: "Falhas consecutivas de batimento: 3"
- Associação marcada como inativa

Causas Possíveis:

- Latência de rede ou perda de pacotes
- PGW-U sobrecarregado
- Intervalo de batimento muito agressivo

Resolução:

O período de batimento é fixo em 5 segundos com um limite de falha de 3 batimentos perdidos consecutivos.

3. Falha no Estabelecimento de Sessão

Sintomas:

- Resposta de Criação de Sessão com código de erro
- Log: "Falha no Estabelecimento de Sessão PFCP"

Causas Possíveis:

- Nenhum par PGW-U disponível
- Exaustão de recursos do PGW-U
- Configuração de regra inválida

Verifique:

1. Verifique se pelo menos um par tem `is_associated = true`
2. Verifique os logs do PGW-U para erros
3. Verifique a unicidade do SEID

4. Erros de SEID Duplicados

Sintomas:

- Resposta de Estabelecimento de Sessão: Causa "Contexto de sessão não encontrado"

Causa:

- Colisão de SEID (muito rara)
- Reinicialização do PGW-U sem conhecimento do PGW-C

Resolução:

- Reinicie a associação PFCP (dispara um novo carimbo de tempo de recuperação)
- O PGW-C detectará a reinicialização do PGW-U e limpará as sessões antigas

Monitoramento da Saúde do PFCP

Métricas a Monitorar:

```
# Status de associação do par PFCP
pfcp_peer_associated{peer="PGW-U Primário"} 1

# Sessões PFCP ativas
seid_registry_count 150

# Taxas de mensagens PFCP
rate(sxb_inbound_messages_total[5m])

# Erros PFCP
rate(sxb_inbound_errors_total[5m])

# Falhas de batimento
pfcp_consecutive_heartbeat_failures{peer="PGW-U Primário"} 0
```

Exemplos de Alertas:

```
# Alerta sobre associação inativa
- alert: PFCPAssociationDown
  expr: pfcp_peer_associated == 0
  for: 1m
  annotations:
    summary: "O par PFCP {{ $labels.peer }} está inativo"

# Alerta sobre altas falhas de estabelecimento de sessão
- alert: PFCPSessionEstablishmentFailureHigh
  expr:
rate(sxb_inbound_errors_total{message_type="session_establishment_res
[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Alta taxa de falha de estabelecimento de sessão PFCP"
```

Interface Web - Monitoramento PFCP

OmniPGW fornece duas páginas da Web para monitorar operações PFCP/Sxb em tempo real.

Página de Status de UPF/Parede PFCP

Acesso: `http://<omnipgw-ip>:<web-port>/upf_status`

Objetivo: Monitorar o status da associação PFCP com todos os pares PGW-U configurados

Recursos:

1. Visão Geral do Status do Par

- **Contagem Associada** - Número de pares com associação PFCP ativa
- **Contagem Não Associada** - Número de pares inativos ou não conectados
- Atualiza a cada 2 segundos

2. Informações por Par Para cada par PGW-U configurado:

- **Nome do Par** - Nome amigável da configuração
- **Endereço IP** - IP remoto do PGW-U
- **Status da Associação** - Associado (verde) ou Não Associado (vermelho)
- **ID do Nó** - Identificador do Nó PFCP
- **Carimbo de Tempo de Recuperação** - Último horário de reinicialização do par
- **Período de Batimento** - Intervalo de batimento configurado
- **Batimentos Perdidos Consecutivos** - Contagem atual de falhas
- **Recursos da Função UP** - Capacidades anunciadas pelo PGW-U

3. Detalhes Expansíveis Clique em qualquer par para ver:

- Configuração completa do par
- Bitmap de recursos da função UP
- Carimbos de tempo de associação
- Estado completo do par

Página de Sessões PFCP

Acesso: `http://<omnipgw-ip>:<web-port>/pfcp_sessions`

Objetivo: Ver sessões PFCP ativas entre OmniPGW e PGW-U

Recursos:

1. Contagem de Sessões Ativas

- Número total de sessões PFCP ativas
- Atualiza em tempo real

2. Informações da Sessão Para cada sessão PFCP:

- **Chave da Sessão** - Chave do registro interno

- **ID do Processo** - Identificador do processo da sessão
- **IMSI** - Assinante associado (se disponível)
- **Status** - Estado da sessão

3. Estado Completo da Sessão Visualização expansível mostrando:

- Contexto completo da sessão PFCP
- PDRs, FARs, QERs, BARs (regras de encaminhamento)
- F-SEIDs (identificadores de ponto de extremidade da sessão)
- Associação do par PGW-U

Casos de Uso Operacionais

Monitorar a Saúde da Associação PFCP:

```
1. Abra a página de Status do UPF
2. Verifique se todos os pares mostram "Associado"
3. Verifique se a contagem de batimentos perdidos = 0
4. Se o par mostrar "Não Associado":
   - Verifique a acessibilidade do IP do par
   - Verifique se o par está em execução
   - Verifique o firewall (UDP 8805)
```

Solução de Problemas de Falhas de Estabelecimento de Sessão:

```
1. A sessão do usuário falha ao estabelecer
2. Verifique a página de Sessões do PGW - a sessão existe?
3. Verifique a página de Sessões PFCP - sessão PFCP criada?
4. Se não houver sessão PFCP:
   - Verifique o Status do UPF - algum par está associado?
   - Verifique os logs para erros PFCP
5. Se a sessão PFCP existir:
   - Inspecione PDRs/FARs para verificar regras programadas
   - O problema é provavelmente a jusante (PGW-U ou rede)
```

Verificar Distribuição de Carga do Par:

```
1. Com múltiplos pares PGW-U configurados
2. Verifique a página de Sessões PFCP
3. Verifique se as sessões estão distribuídas entre os pares
4. Identifique se um par tem carga desproporcional
```

Detectar Falhas de Par:

- Olhada rápida na página de Status do UPF
- Distintivo vermelho "Não Associado" imediatamente visível
- Contador de batimentos perdidos mostra degradação antes da falha total
- Configure alertas de monitoramento com base nos dados da Web UI

Vantagens:

- **Monitoramento em tempo real** - Sem necessidade de consultar métricas ou SSH
- **Status visual** - Código de cores associado/não associado
- **Tendências de saúde do par** - Contagem de batimentos perdidos mostra aviso antecipado
- **Inspeção em nível de sessão** - Veja exatamente PDRs/FARs/QERs programados
- **Sem ferramentas necessárias** - Apenas um navegador da Web

---

Documentação Relacionada

Configuração

- **Guia de Configuração** - Seleção de UPF, monitoramento de saúde, configuração PFCP
- **Gerenciamento de Sessão** - Ciclo de vida da sessão PDN, estabelecimento de bearer

Cobrança e Monitoramento

- **Interface Diameter Gx** - Regras PCC que impulsionam a aplicação de QoS PFCP
- **Interface Diameter Gy** - Gerenciamento de cotas de cobrança online via URRs
- **Formato de CDR de Dados** - Geração de CDR a partir de relatórios de uso PFCP
- **Guia de Monitoramento** - Métricas PFCP, rastreamento de sessões, alertas de saúde do UPF

Interfaces de Rede

- **Interface S5/S8** - Gerenciamento de bearer do plano de controle
- **Alocação de IP do UE** - Atribuição de endereço do UE via PFCP

Voltar ao Guia de Operações

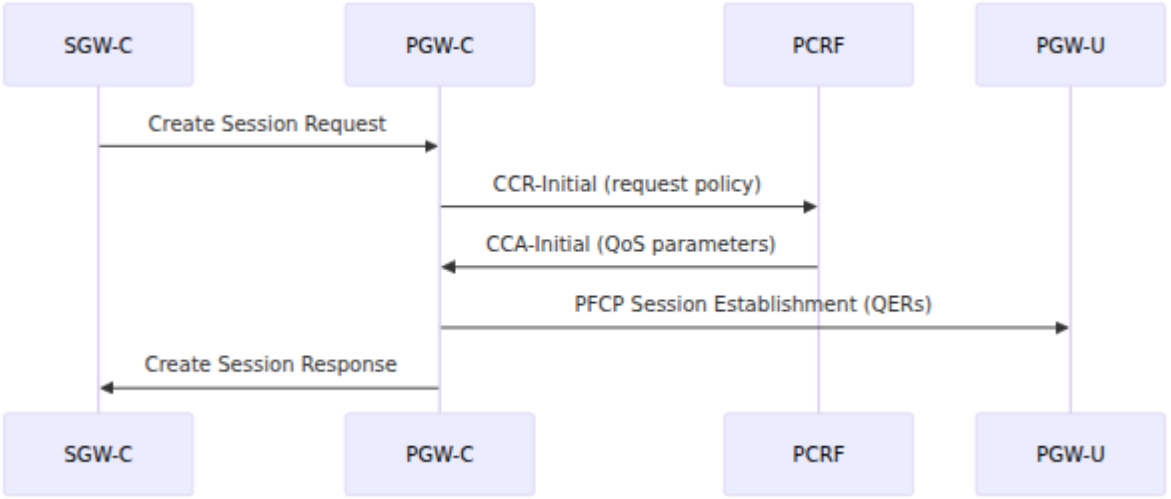
QoS & Gerenciamento de Bearer

Visão Geral

O PGW-C implementa um sistema de gerenciamento de bearer e QoS orientado por políticas que coordena três interfaces principais:

- **Gx (Diameter)** - Recebe decisões de política e parâmetros de QoS do PCRF
- **S5/S8 (GTP-C)** - Gerencia contextos de bearer com SGW-C
- **Sxb (PFCP)** - Programa regras de aplicação de QoS no PGW-U

Fluxo da Arquitetura



Conceitos Chave

- **Sessão**: Contém informações do UE, mapa de bearer, mapas de PDR/FAR/QER/BAR e AMBR
- **Contexto de Bearer**: Liga EBI (EPS Bearer ID) a PDRs, FARs e QERs específicos

- **QER (Regra de Aplicação de QoS)**: Impõe limites de MBR/GBR e status de gate no plano do usuário
- **Bearer Padrão**: Sempre criado com a sessão PDN, fornece conectividade básica
- **Bearer Dedicado**: Criado dinamicamente com base na política do PCRF, fornece garantias específicas de QoS

Configuração

Importante: Política de QoS Dinâmica

Todos os parâmetros de QoS são recebidos dinamicamente do PCRF via interface Diameter Gx e definidos no PCRF (Veja OmniHSS para mais informações).

Os operadores configuram a **conexão PCRF** em `config/runtime.exs`:

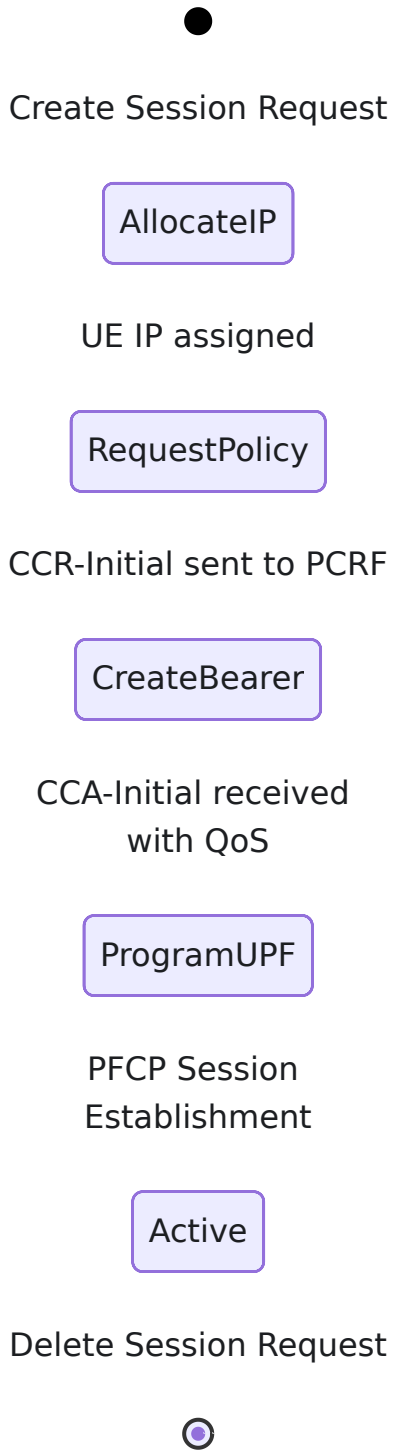
```
config :pgw_c,
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "192.168.1.100",
        initiate_connection: true
      }
    ]
  }
```

Políticas de QoS, regras de cobrança e limites de largura de banda são configurados no PCRF, não nos arquivos de configuração do PGW-C.

Ciclo de Vida do Bearer

Criação do Bearer Padrão

O bearer padrão é criado durante o estabelecimento da sessão PDN:



Fluxo de Trabalho:

1. SGW-C envia Create Session Request
2. PGW-C aloca o endereço IP do UE do pool configurado
3. PGW-C envia CCR-Initial ao PCRF com IMSI, APN, endereço IP
4. PCRF responde com CCA-Initial contendo parâmetros de QoS:
    - Default-EPS-Bearer-QoS (QCI, ARP)
    - QoS-Information (ajustes de AMBR)
5. PGW-C cria contexto de bearer com:
    - IDs fixos: Downlink PDR=1, Uplink PDR=2, Downlink FAR=1, Uplink FAR=2, QER=1, BAR=1
    - QER programado com MBR do QoS do bearer
6. PGW-C envia PFCP Session Establishment Request para PGW-U
7. PGW-C envia Create Session Response para SGW-C

Características do bearer padrão:

- Sempre existe durante a vida útil da sessão PDN
- Normalmente usa QCI 5 ou QCI 9 (não-GBR)
- EBI rastreado no estado da sessão
- Não pode ser excluído independentemente (excluí-lo termina a sessão)

Criação do Bearer Dedicado

Bearers dedicados são criados dinamicamente com base na política do PCRF:

Gatilho: Re-Auth Request (RAR) do PCRF com Charging-Rule-Install

Fluxo de Trabalho:

1. PCRF envia RAR com Charging-Rule-Definition contendo:
    - Charging-Rule-Name (identificador da regra de política)
    - Flow-Information (filtros de pacotes)
    - QoS-Information (QCI, MBR, GBR, ARP)
    - Precedence (prioridade de correspondência da regra)
2. PGW-C traduz a regra dinâmica para entidades PFCP:
    - Cada entrada de Flow-Information → novo PDR com SDF Filter
    - QoS-Information → novo QER com aplicação de MBR/GBR

    - Flow-Description → regras de correspondência de IP 5-tuple
3. PGW-C envia PFCP Session Modification Request para adicionar PDRs/FARs/QERs
4. PGW-C inicia Create Bearer Request para SGW-C
5. SGW-C responde com Create Bearer Response confirmando o estabelecimento

Exemplo de Charging-Rule-Definition:

```
Charging-Rule-Name: "video_streaming"
Flow-Information:
  - Flow-Description: "permit in ip from any to 10.0.0.1 5000-
6000"
    Flow-Direction: 1 (downlink)
QoS-Information:
  QoS-Class-Identifier: 7
  Max-Requested-Bandwidth-UL: 5000000 (5 Mbps)
  Max-Requested-Bandwidth-DL: 10000000 (10 Mbps)
  Guaranteed-Bitrate-UL: 1000000 (1 Mbps)
  Guaranteed-Bitrate-DL: 2000000 (2 Mbps)
Precedence: 100
Flow-Status: 2 (ENABLED)
```

Modificação do Bearer

A QoS do bearer pode ser modificada via:

- **Gx RAR** com a Charging-Rule-Definition atualizada
- **PFCP Session Modification** para atualizar QERs existentes (alterar bitrates), FARs (alterar encaminhamento) ou PDRs (alterar filtros de pacotes)

Exclusão do Bearer

Gatilhos:

- **Delete Session Request** (iniciado pelo SGW) - Exclui o bearer padrão e termina a sessão

- **Re-Auth Request com Charging-Rule-Remove** (iniciado pelo PCRF) - Exclui o bearer dedicado

Fluxo de Trabalho:

1. Remover bearer do estado da sessão
2. Remover PDRs/FARs/QERs associados
3. Enviar Delete Bearer Request para SGW-C (se iniciado pelo PCRF)
4. Enviar PFCP Session Modification (remover regras) ou Session Deletion (se bearer padrão)

Parâmetros de QoS

QCI (Identificador de Classe de QoS)

Fonte: PCRF via Gx `QoS-Class-Identifier` AVP

Valores Padrão:

- **QCI 1**: Voz Conversacional (GBR, 100ms de orçamento de atraso)
- **QCI 2**: Vídeo Conversacional (GBR, 150ms de orçamento de atraso)
- **QCI 3**: Jogos em Tempo Real (GBR, 50ms de orçamento de atraso)
- **QCI 4**: Vídeo Não Conversacional (GBR, 300ms de orçamento de atraso)
- **QCI 5**: Sinalização IMS (não-GBR, 100ms de orçamento de atraso) - **Padrão para bearer padrão**
- **QCI 6**: Vídeo (baseado em TCP), Streaming Ao Vivo (não-GBR, 300ms de orçamento de atraso)
- **QCI 7**: Voz, Jogos Interativos (não-GBR, 100ms de orçamento de atraso)
- **QCI 8**: Vídeo (baseado em TCP), por exemplo, YouTube (não-GBR, 300ms de orçamento de atraso)
- **QCI 9**: Internet Padrão (não-GBR, 300ms de orçamento de atraso)

Nota do Operador:

- O QCI é recebido do PCRF e sinalizado para SGW-C no Bearer-Level-QoS IE

- O PGW-C não aplica diretamente o comportamento do QCI - a aplicação real é via MBR/GBR nos QERs
- Valores de QCI mais baixos geralmente indicam maior prioridade
- O QCI determina o tratamento de encaminhamento de pacotes e a prioridade de agendamento

ARP (Prioridade de Alocação e Retenção)

Fonte: PCRF via `Allocation-Retention-Priority` grouped AVP

Componentes:

- **Priority-Level**: 1 (maior prioridade) a 15 (menor prioridade)
- **Pre-emption-Capability**: Este bearer pode preemptar bearers de menor prioridade?
  - 0 = HABILITADO (pode preemptar outros)
  - 1 = DESABILITADO (não pode preemptar)
- **Pre-emption-Vulnerability**: Este bearer pode ser preemptado por bearers de maior prioridade?
  - 0 = HABILITADO (pode ser preemptado)
  - 1 = DESABILITADO (não pode ser preemptado)

Valores Padrão:

- Priority-Level: 1
- Pre-emption-Capability: HABILITADO (0)
- Pre-emption-Vulnerability: DESABILITADO (1)

Nota do Operador:

- O ARP é sinalizado para SGW-C e, em última instância, para eNodeB
- **Não é aplicado pelo PGW-C** - a aplicação é tipicamente no eNodeB durante o controle de admissão de rádio
- Usado durante a congestão da rede para determinar quais bearers admitir ou descartar
- Crítico para serviços de emergência (nível de prioridade 1) e serviços de alto valor

MBR (Taxa Máxima de Bits)

Fonte: PCRF via `Max-Requested-Bandwidth-UL` e `Max-Requested-Bandwidth-DL` AVPs

Formato: Bytes por segundo (convertido para kbps internamente: `bytes / 1000`)

Aplicado a: Todos os bearers (padrão e dedicado)

Como funciona:

- O PGW-C cria QER com `mbr: %Bitrate{ul: kbps_ul, dl: kbps_dl}`
- QER enviado para PGW-U via PFCP
- **PGW-U aplica limitação de taxa** (policiamento de tráfego)
- Tráfego excessivo acima do MBR é descartado

Exemplo:

```
Max-Requested-Bandwidth-UL: 5000000 (5 Mbps)
Max-Requested-Bandwidth-DL: 10000000 (10 Mbps)

→ QER criado com mbr: {ul: 5000, dl: 10000} kbps
→ PGW-U descarta pacotes de uplink que excedem 5 Mbps
→ PGW-U descarta pacotes de downlink que excedem 10 Mbps
```

GBR (Taxa de Bits Garantida)

Fonte: PCRF via `Guaranteed-Bitrate-UL` e `Guaranteed-Bitrate-DL` AVPs

Formato: Bytes por segundo (convertido para kbps)

Aplicado a: Apenas bearers dedicados (bearers GBR)

Como funciona:

- Se GBR for especificado na Charging-Rule-Definition, o bearer é **do tipo GBR**
- O PGW-U aplica a garantia de taxa mínima via QER

- Requer agendamento adequado no eNodeB para reservar recursos de rádio
- Bearers GBR têm controle de admissão - podem ser rejeitados se os recursos não estiverem disponíveis

Exemplo:

```
Guaranteed-Bitrate-UL: 1000000 (1 Mbps)
Guaranteed-Bitrate-DL: 2000000 (2 Mbps)

→ QER criado com gbr: {ul: 1000, dl: 2000} kbps
→ A rede garante pelo menos 1 Mbps de uplink e 2 Mbps de downlink
→ Usado para VoIP, chamadas de vídeo, streaming ao vivo
```

Nota do Operador:

- GBR requer planejamento de capacidade de rede suficiente
- Sobrecarga de recursos GBR leva a falhas de admissão
- Monitorar o uso de GBR via contagem de sessões e métricas de bearers

AMBR (Taxa Máxima Agregada de Bits)

Fonte: PCRF via `APN-Aggregate-Max-Bitrate-UL` e `APN-Aggregate-Max-Bitrate-DL` AVPs

Escopo: Aplica-se a **todos os bearers não-GBR** para o APN (não por bearer)

Como funciona:

- AMBR é um limite agregado em todos os bearers não-GBR em uma sessão
- Enviado para SGW-C na Create Session Response
- A aplicação é tipicamente no eNodeB/SGW
- PGW-C armazena AMBR no estado da sessão e sinaliza para SGW-C

Exemplo:

```
APN-Aggregate-Max-Bitrate-UL: 50000000 (50 Mbps)
APN-Aggregate-Max-Bitrate-DL: 100000000 (100 Mbps)

→ Todos os bearers não-GBR combinados não podem exceder 50 Mbps de
uplink / 100 Mbps de downlink
→ Bearers individuais limitados pelo seu próprio MBR
→ AMBR fornece um limite adicional geral por UE/APN
```

Nota do Operador:

- Definido via perfil de assinante no HSS/PCRF
- Usado para aplicar níveis de assinatura (por exemplo, plano de 10 Mbps vs plano de 100 Mbps)
- Não afeta bearers GBR

Status do Fluxo e Controle de Acesso

Mapeamento de Status do Fluxo (Gx) para Status do Gate (PFCP)

O PCRF controla se o tráfego é permitido via o AVP `Flow-Status` na Charging-Rule-Definition:

Flow-Status (Gx)	Gate-Status (PFCP QER)	Significado
0 = ENABLED-UPLINK	ul: OPEN, dl: CLOSED	Apenas tráfego de uplink permitido
1 = ENABLED-DOWNLINK	ul: CLOSED, dl: OPEN	Apenas tráfego de downlink permitido
2 = ENABLED	ul: OPEN, dl: OPEN	Ambas as direções permitidas
3 = DISABLED	ul: CLOSED, dl: CLOSED	Nenhum tráfego permitido
4 = REMOVED	ul: CLOSED, dl: CLOSED	Bearer sendo excluído

Casos de uso:

- **DISABLED**: Usado para serviços estacionados ou exaustão de crédito (pacotes descartados, mas bearer mantido)
- **ENABLED-UPLINK**: Incomum, mas pode ser usado para serviços apenas de upload
- **ENABLED-DOWNLINK**: Serviços apenas de download ou cenários com crédito limitado
- **ENABLED**: Operaç��o normal

Monitoramento & Observabilidade

Métricas do Prometheus

Métricas de nível de sessão:

```
session_registry_count        # Bearers ativos (pares IMSI, EBI)
address_registry_count        # IPs do UE alocados
charging_id_registry_count    # Sessões de cobrança ativas
```

Métricas da interface Gx:

```
gx_inbound_messages_total{message_type="gx_RAR"}     #
Atualizações de política do PCRF
gx_outbound_messages_total{message_type="gx_CCR"}    #
Solicitações de política ao PCRF
gx_outbound_transaction_duration_bucket              # Latência ao
PCRF
```

Métricas da interface PFCP:

```
sxb_outbound_messages_total{message_type="pfcp_session_establishment_
sxb_outbound_messages_total{message_type="pfcp_session_modification_r
sxb_outbound_transaction_duration_bucket
```

Métricas de criação de bearer:

```
s5s8_inbound_messages_total{message_type="create_session_request"}
# Bearers padrão
s5s8_outbound_messages_total{message_type="create_bearer_request"}
# Bearers dedicados
```

Monitoramento da Interface Web

Página de Sessões PGW (`/pgw_sessions`):

- Pesquisar por IMSI, endereço IP, MSISDN ou APN
- Visualizar bearers ativos por sessão
- Inspecionar parâmetros de QoS do bearer (QCI, MBR, GBR, AMBR)
- Atualização automática em tempo real (2 segundos)

Página Diameter (`/diameter`):

- Status de conectividade do par PCRF
- Contagem de sessões Gx
- Estado do par (conectado/desconectado)

Página de Logs (`/logs`):

- Streaming de logs em tempo real
- Filtrar por "Controle de Crédito" para trocas CCR/CCA
- Filtrar por "Re-Auth" para eventos RAR (mudanças de política)
- Filtrar por "PFCP" para eventos de programação do plano do usuário

Mensagens de Log Chave

```
[debug] Sending Credit Control Request: ...          # CCR para
PCRF
[debug] Handling Credit Control Answer: ...          # CCA do PCRF
(contém QoS)
[debug] Handling Re-Auth Request                     # RAR do PCRF
(mudança de política)
[debug] Sending Session Establishment Request        # PFCP para
PGW-U (programar QERs)
[debug] Sending Session Modification Request         # PFCP para
PGW-U (atualizar QERs)
```

Tarefas Operacionais

Verificar QoS Aplicada à Sessão

1. Acesse a Interface Web → página **PGW Sessions**
2. Pesquise por IMSI (por exemplo, `999000123456789`)
3. Expanda os detalhes da sessão
4. Verifique a seção **qer_map**:

```
qer_id: 1
gate_status: {ul: OPEN, dl: OPEN}
mbr: {ul: 50000, dl: 100000}  # kbps
gbr: {ul: 10000, dl: 20000}   # kbps (ou nil para não-GBR)
```

5. Verifique se os valores correspondem à política esperada do PCRF

Solucionar Problemas de QoS Ausente

Sintoma: Sessão criada, mas QoS não aplicada

Passos:

1. **Verifique a conectividade do PCRF:**
   - Acesse a Interface Web → página **Diameter**
   - Verifique se o status do par PCRF = "conectado"
   - Se desconectado, verifique a conectividade da rede e a configuração do Diameter
2. **Verifique a troca CCR/CCA:**
   - Acesse a Interface Web → página **Logs**
   - Pesquise por "Credit Control Answer"
   - Verifique se o AVP `QoS-Information` está presente no log da CCA
   - Verifique se há erros na CCA (Result-Code deve ser 2001 = SUCESSO)
3. **Verifique a programação do PFCP:**
   - Pesquise logs por "PFCP Session Establishment Request"
   - Verifique se o QER está incluído na mensagem
   - Verifique os logs do PGW-U para erros de processamento do PFCP
4. **Verifique a configuração da política do PCRF:**
   - Verifique o perfil do assinante no PCRF
   - Confirme se as regras de política específicas do APN existem
   - Verifique os logs do PCRF para erros de avaliação de política

Monitorar Taxa de Criação de Bearer

Consultas do Prometheus:

```
# Taxa de criação de bearer padrão (sessões/segundo)
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])

# Taxa de criação de bearer dedicado
rate(s5s8_outbound_messages_total{message_type="create_bearer_request
[5m])

# Taxa de atualização de política do PCRF
rate(gx_inbound_messages_total{message_type="gx_RAR"}[5m])
```

Planejamento de Capacidade

Métricas chave a serem monitoradas:

```
# Utilização do endereço IP do UE (porcentagem)
(address_registry_count / <configured_pool_size>) * 100

# Contagem de bearers ativos
session_registry_count

# Latência da consulta do PCRF (P95)
histogram_quantile(0.95, gx_outbound_transaction_duration_bucket)
```

Limites de capacidade:

- Tamanho do pool de endereços: configurado em `config/runtime.exs` sob `ue.subnet_map`
- Espaço TEID: 32 bits (4 bilhões de identificadores únicos, gerenciados automaticamente)
- Sessões concorrentes: tipicamente limitadas pelo tamanho do pool de endereços

Diretrizes de planejamento:

- Monitore a utilização de endereços IP - amplie o pool antes de exceder 80%
- Monitore a latência do PCRF - alta latência impacta o tempo de configuração da sessão
- Monitore a taxa de criação de bearers dedicados - indica a complexidade da política

Documentação Relacionada

- Gerenciamento de Sessão - Ciclo de vida da sessão PDN
- Interface Diameter Gx - Detalhes do protocolo de política do PCRF
- Interface PFCP - Programação do plano do usuário
- Guia de Configuração - Configuração do sistema
- Guia de Monitoramento - Métricas e observabilidade

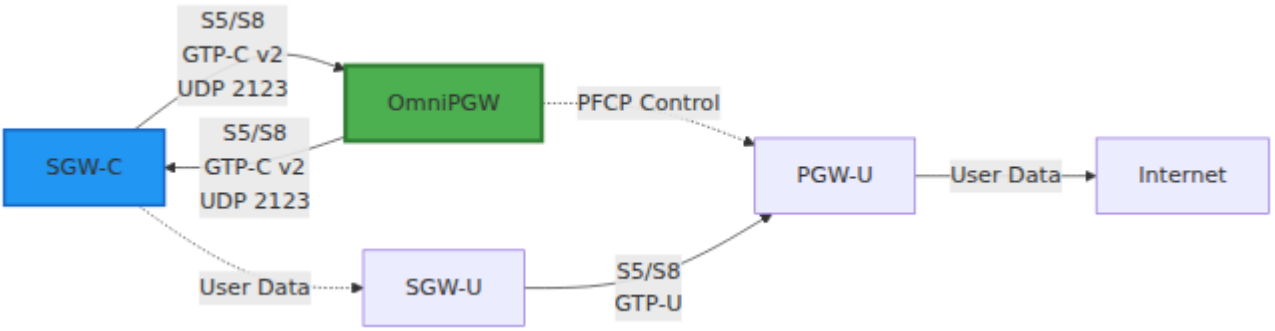
Documentação da Interface S5/S8

Comunicação GTP-C com SGW-C

OmniPGW da Omnitouch Network Services

Visão Geral

A **interface S5/S8** conecta o OmniPGW ao SGW-C (Serviço de Controle de Gateway) usando o protocolo **GTP-C v2** (Protocolo de Tunelamento GPRS - Plano de Controle). Esta interface gerencia o sinalização de gerenciamento de sessão entre os gateways.



Detalhes do Protocolo

GTP-C Versão 2

- **Protocolo:** GTP-C v2 (3GPP TS 29.274)
- **Transporte:** UDP
- **Porta:** 2123 (padrão)
- **Tipo de Interface:** Plano de Controle

TEID (Identificador de Ponto de Extremidade do Túnel)

Cada sessão tem um **TEID** único para roteamento de mensagens:

- **TEID Local** - Alocado pelo OmniPGW para mensagens de entrada
- **TEID Remoto** - Alocado pelo SGW-C para mensagens de saída

```
Fluxo de Mensagem:
  SGW-C → OmniPGW: TEID de Destino = TEID Local do OmniPGW
  OmniPGW → SGW-C: TEID de Destino = TEID Remoto do SGW-C
```

Configuração

Configuração Básica

```
# config/runtime.exs
config :pgw_c,
  s5s8: %{
    # Endereço IPv4 local para a interface S5/S8
    local_ipv4_address: "10.0.0.20",

    # Opcional: Endereço IPv6 local
    local_ipv6_address: nil,

    # Opcional: Substituir porta padrão
    local_port: 2123,

    # Tempo limite de requisição GTP-C em milissegundos (padrão:
500ms)
    # Tempo limite por tentativa ao aguardar respostas GTP-C
(Criar Bearer, Deletar Bearer, etc.)
    request_timeout_ms: 500,

    # Número de tentativas de reenvio para requisições GTP-C
(padrão: 3)
    # Tempo máximo total de espera = request_timeout_ms *
request_attempts
    # Exemplo: 500ms * 3 tentativas = 1500ms (1,5 segundos) total
    request_attempts: 3
  }
```

Configuração de Timeout

A interface S5/S8 utiliza timeouts configuráveis para transações de requisição/resposta GTP-C.

Parâmetros:

- **`request_timeout_ms`** - Timeout em milissegundos por tentativa de reenvio (padrão: 500ms)

- **`request_attempts`** - Número de tentativas de reenvio antes de desistir (padrão: 3)

Tempo Total de Espera: `request_timeout_ms × request_attempts`

Comportamento padrão: 500ms × 3 tentativas = **1,5 segundos de espera máxima total**

Diretrizes de Ajuste:

Latência da Rede	`request_timeout_ms` Recomendado	Tempo Total de Espera
Baixa latência (<50ms)	200-300ms	600-900ms (3 tentativas)
Normal (50-150ms)	500ms (padrão)	1,5s (3 tentativas)
Alta latência (>150ms)	1000-2000ms	3-6s (3 tentativas)
Instável/satélite	2000-3000ms	6-9s (3 tentativas)

Exemplo - Rede de Alta Latência:

```
s5s8: %{
  local_ipv4_address: "10.0.0.20",
  request_timeout_ms: 1500,  # 1,5 segundos por tentativa
  request_attempts: 3         # Total: 4,5 segundos no máximo
}
```

Quando ocorre timeout:

- OmniPGW registra erro: `"Tempo limite da Requisição de Criação de Bearer"`
- Retorna erro ao PCRF (Código de Resultado Diameter: 5012 UNABLE_TO_COMPLY)

- Bearer permanece em armazenamento inicial para limpeza via Charging-Rule-Remove

Requisitos de Rede

Regras de Firewall:

```
# Permitir GTP-C da rede SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_network>/24 -j
ACCEPT

# Permitir GTP-C de saída para SGW-C
iptables -A OUTPUT -p udp --dport 2123 -d <sgw_network>/24 -j
ACCEPT
```

Roteamento:

```
# Garantir rota para a rede SGW-C
ip route add <sgw_network>/24 via <gateway_ip> dev eth0
```

Tipos de Mensagens

A interface S5/S8 gerencia a sinalização GTP-C para gerenciamento de sessão PDN. Para um ciclo de vida de sessão detalhado e gerenciamento de estado, consulte o Guia de Gerenciamento de Sessão.

Gerenciamento de Sessão

Requisição de Criação de Sessão

Direção: SGW-C → OmniPGW

Propósito: Estabelecer uma nova conexão PDN

Principais IEs (Elementos de Informação):

Nome do IE	Tipo	Descrição
IMSI	Identidade	Identidade Internacional do Assinante Móvel
MSISDN	Identidade	Número de telefone móvel
APN	String	Nome do Ponto de Acesso (ex: "internet")
Tipo de RAT	Enum	Tecnologia de Acesso Rádio (EUTRAN)
Contexto de Bearer	Agrupado	Informações do bearer padrão
Fuso Horário do UE	Timestamp	Fuso horário do UE
ULI	Agrupado	Informações de Localização do Usuário (TAI, ECGI)
Rede Servidora	PLMN	MCC/MNC da rede servidora

Exemplo:

```
Requisição de Criação de Sessão
├── IMSI: 310260123456789
├── MSISDN: 14155551234
├── APN: internet
├── Tipo de RAT: EUTRAN (6)
├── Contexto de Bearer
│   ├── EBI: 5
│   ├── QoS do Bearer (QCI 9, ARP, taxas de bits)
│   └── S5/S8 F-TEID (ponto de extremidade do túnel SGW-U)
└── ULI
    ├── TAI: MCC 310, MNC 260, TAC 12345
    └── ECGI: MCC 310, MNC 260, ECI 67890
```

Resposta de Criação de Sessão

Direção: OmniPGW → SGW-C

Propósito: Reconhecer a criação da sessão

Principais IEs:

Nome do IE	Tipo	Descrição
Causa	Resultado	Código de sucesso ou erro
Contexto de Bearer	Agrupado	Informações do bearer
Alocação de Endereço PDN	IP	Endereço IP alocado para o UE (veja Alocação de IP do UE)
Restrição de APN	Enum	Restrições de uso do APN
PCO	Opções	Opções de Configuração de Protocolo (veja Configuração PCO)

Resposta de Sucesso:

```
Resposta de Criação de Sessão
├── Causa: Requisição aceita (16)
├── Alocação de Endereço PDN
│   └── IPv4: 100.64.1.42
├── Contexto de Bearer
│   ├── EBI: 5
│   ├── Causa: Requisição aceita
│   └── S5/S8 F-TEID (ponto de extremidade do túnel PGW-U do PFCP)
├── Restrição de APN: Público-1 (1)
└── PCO
    ├── Servidor DNS: 8.8.8.8
    ├── Servidor DNS: 8.8.4.4
    └── MTU do Link: 1400
```

Requisição de Deleção de Sessão

Direção: SGW-C → OmniPGW

Propósito: Terminar a conexão PDN

Principais IEs:

Nome do IE	Descrição
EBI	ID do Bearer EPS a ser deletado
EBI Vinculado	Bearer relacionado (opcional)

Resposta de Deleção de Sessão

Direção: OmniPGW → SGW-C

Propósito: Reconhecer a deleção da sessão

Principais IEs:

Nome do IE	Descrição
Causa	Código de sucesso ou erro

Gerenciamento de Bearer

Requisição de Criação de Bearer

Direção: OmniPGW → SGW-C

Propósito: Criar bearer dedicado (iniciado pela política do PCRF)

Acionado por:

- PCRF envia nova regra PCC exigindo bearer dedicado
- OmniPGW solicita ao SGW-C para estabelecer o bearer

Requisição de Deleção de Bearer

Direção: OmniPGW → SGW-C ou SGW-C → OmniPGW

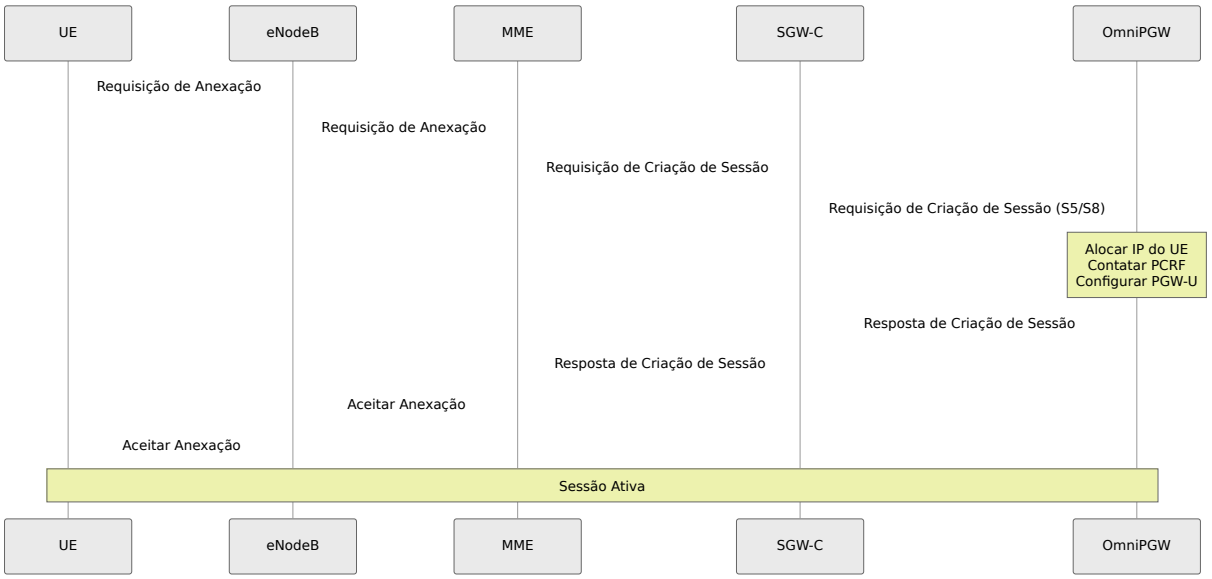
Propósito: Deletar bearer dedicado

Cenários:

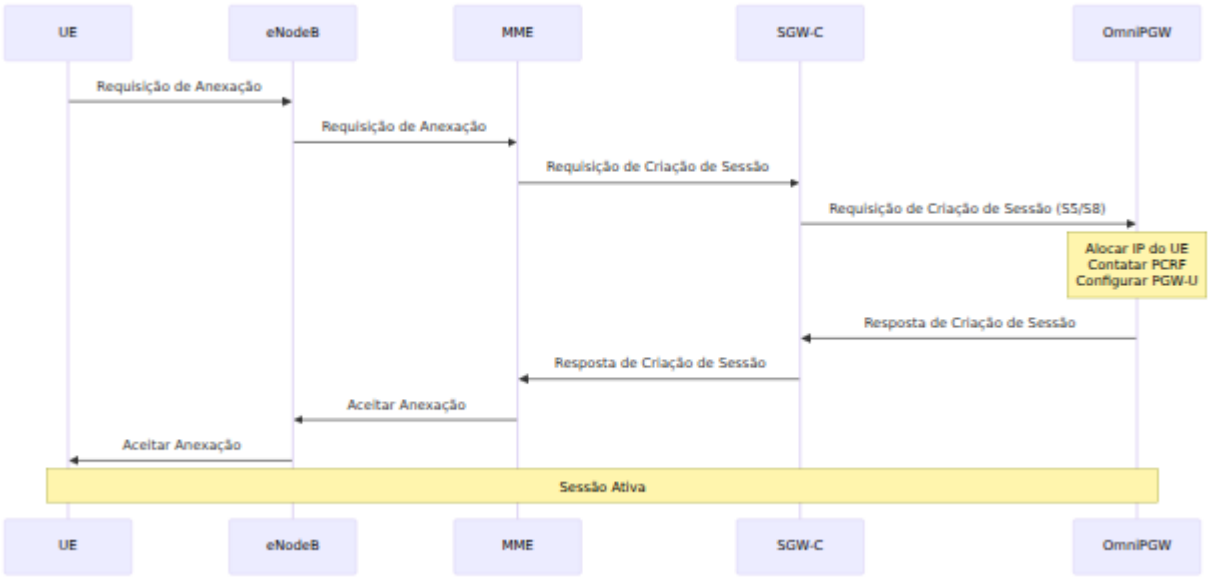
- **Iniciado pelo PGW:** Mudança de política do PCRF remove bearer dedicado
- **Iniciado pelo SGW:** Liberação de recursos de rádio

Fluxos de Mensagem

Estabelecimento de Sessão



Término de Sessão



Códigos de Causa

Sucesso

Código	Nome	Descrição
16	Requisição aceita	Operação bem-sucedida

Erros (Falhas Permanentes)

Código	Nome	Quando Usado
65	Usuário Desconhecido	PCRF rejeitou (IMSI não encontrado)
66	Recursos não disponíveis	Pool de IP esgotado
93	Serviço não suportado	APN inválido
94	Erro semântico no TFT	Modelo de fluxo de tráfego inválido

Erros (Falhas Transitórias)

Código	Nome	Quando Usado
72	Par remoto não respondendo	Timeout do PCRF/PGW-U
73	Colisão com requisição iniciada pela rede	Operações simultâneas

---

Monitoramento

Métricas S5/S8

```
# Contadores de mensagens
s5s8_inbound_messages_total{message_type="create_session_request"}
s5s8_inbound_messages_total{message_type="delete_session_request"}

# Contadores de erro
s5s8_inbound_errors_total

# Latência de manuseio de mensagens
s5s8_inbound_handling_duration_bucket

# TEIDs ativos
teid_registry_count
```

Consultas Úteis

Taxa de Criação de Sessão:

```
rate(s5s8_inbound_messages_total{message_type="create_session_request
[5m])
```

Taxa de Erro:

```
rate(s5s8_inbound_errors_total[5m])
```

Latência (p95):

```
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Solução de Problemas

Problema: Sem Resposta do OmniPGW

Sintomas:

- SGW-C envia Requisição de Criação de Sessão
- Nenhuma resposta recebida
- Timeout no SGW-C

Causas:

1. Problema de conectividade de rede
2. OmniPGW não está ouvindo no IP configurado
3. Firewall bloqueando UDP 2123
4. TEID incorreto na requisição

Depuração:

```
# Verificar se o OmniPGW está ouvindo
netstat -ulnp | grep 2123

# Verificar pacotes de entrada
tcpdump -i any -n port 2123

# Verificar configuração
grep "local_ipv4_address" config/runtime.exs

# Verificar firewall
iptables -L -n | grep 2123
```

Problema: Falha na Criação de Sessão

Sintomas:

- Resposta de Criação de Sessão com causa de erro
- Sessão não estabelecida

Causas Comuns:

```
Causa 65 (Usuário Desconhecido):
  → PCRF rejeitou assinante
  → Verificar IMSI no HSS/SPR

Causa 66 (Sem recursos):
  → Pool de IP esgotado
  → Verificar: curl http://pgw:9090/metrics | grep
address_registry_count
  → Expandir pool de IP

Causa 72 (Par remoto não respondendo):
  → Timeout do PCRF ou PGW-U fora do ar
  → Verificar conectividade Gx
  → Verificar associação PFCP
```

Problema: Colisão de TEID

Sintomas:

- Mensagem roteada para a sessão errada
- Comportamento inesperado

Causa:

- TEID reutilizado antes da limpeza
- Bug na alocação de TEID

Resolução:

- Garantir alocação única de TEID
- Verificar registro de TEID para vazamentos

Melhores Práticas

Design de Rede

1. **Interface de Rede Dedicada**
    - Usar VLAN separada para S5/S8
    - Isolar do tráfego de gerenciamento
2. **Otimização de MTU**
    - Garantir que o MTU suporte cabeçalhos GTP
    - MTU mínima: 1500 bytes (1464 carga útil + 36 GTP)
3. **Redundância**
    - Múltiplas instâncias do OmniPGW
    - Balanceamento de carga baseado em DNS do SGW-C

Desempenho

1. **Tamanhos de Buffer UDP**
    - Aumentar buffers de socket para alta carga

- Típico: 4-8 MB por socket

2. **Limites de Conexão**
   - Planejar para contagem de sessão esperada
   - Monitorar contagem de registro de TEID

Segurança

1. **Filtragem de IP**
   - Permitir apenas GTP-C de IPs SGW-C conhecidos
   - Usar iptables ou ACLs de rede

2. **Validação de Mensagens**
   - OmniPGW valida todas as mensagens recebidas
   - Rejeita pacotes GTP-C malformados

Documentação Relacionada

Funções Principais

- **Guia de Configuração** - Configuração da interface S5/S8, configuração de IP local
- **Gerenciamento de Sessão** - Ciclo de vida da sessão PDN, estabelecimento de bearer
- **Alocação de IP do UE** - Entrega de endereço IP via Resposta de Criação de Sessão
- **Configuração PCO** - Parâmetros PCO em mensagens GTP-C

Interfaces Relacionadas

- **Interface Gn/Gp** - GTP-C v1 para funcionalidade GGSN 2G/3G

- **Interface PFCP** - Coordenação do plano de usuário com o plano de controle S5/S8
- **Interface Diameter Gx** - Integração de políticas com configuração de bearer
- **Interface Diameter Gy** - Integração de cobrança com gerenciamento de bearer

Operações

- **Guia de Monitoramento** - Métricas GTP-C S5/S8, rastreamento de mensagens
- **Formato de CDR de Dados** - Geração de CDR a partir de sessões GTP-C

Voltar ao Guia de Operações

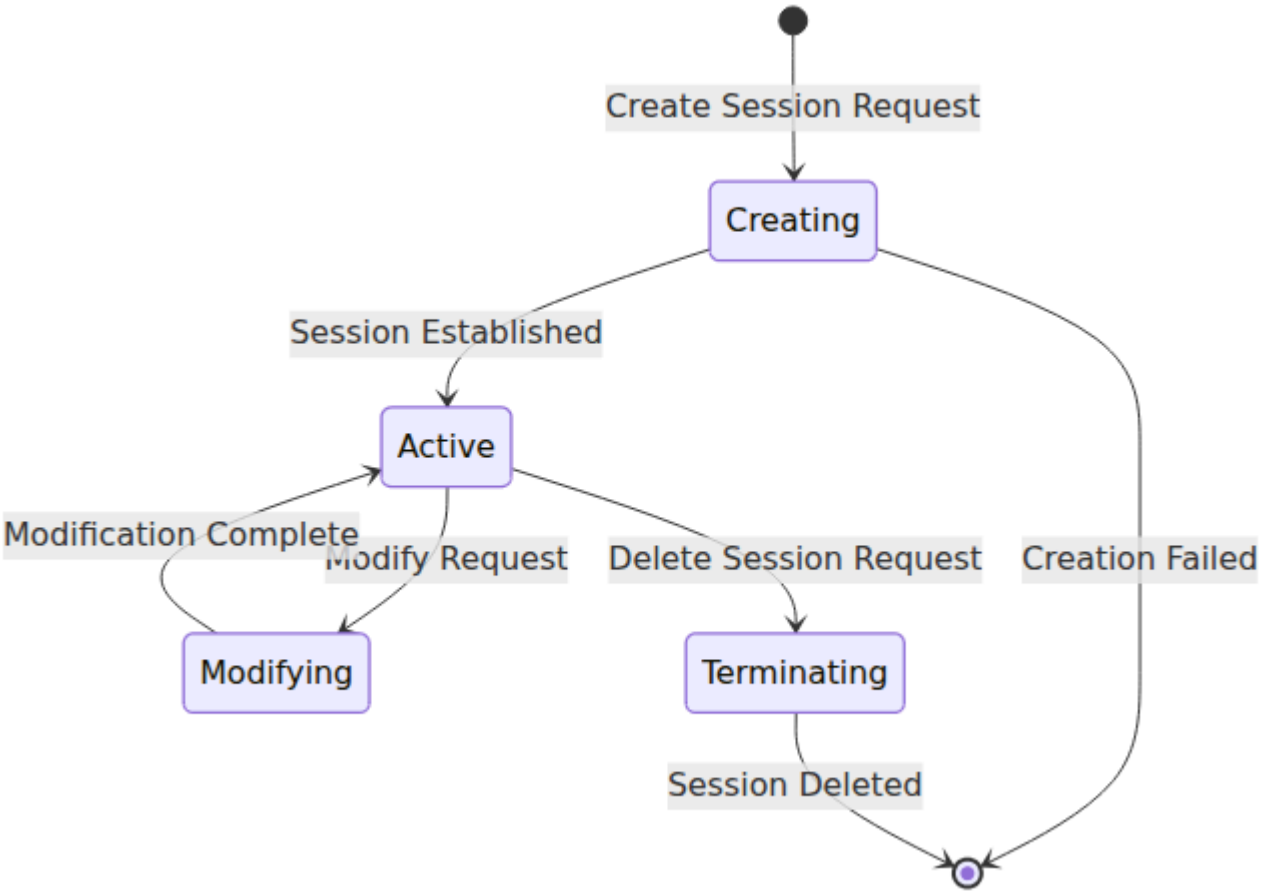
Guia de Gerenciamento de Sessão

Ciclo de Vida e Operações da Conexão PDN

OmniPGW da Omnitouch Network Services

Visão Geral

Uma **Sessão PDN (Packet Data Network)** representa a conexão de dados de um UE através do OmniPGW. Cada sessão coordena múltiplas interfaces e recursos para habilitar a conectividade de dados.



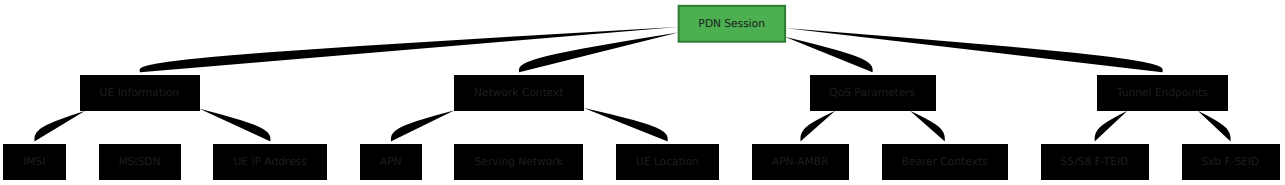
Componentes da Sessão

Identificadores da Sessão

Cada sessão possui múltiplos identificadores para diferentes interfaces:

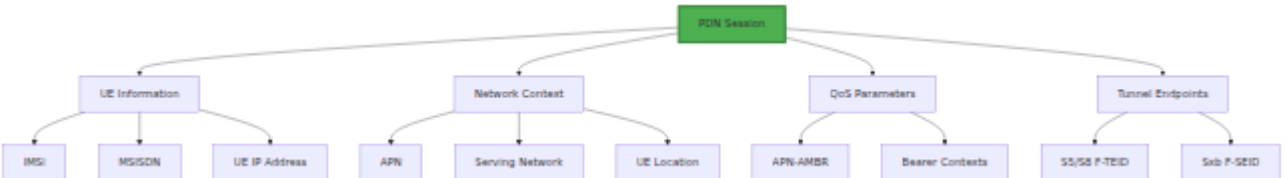
Identificador	Interface	Propósito
TEID	S5/S8 (GTP-C)	Tunnel Endpoint ID para comunicação SGW-C
SEID	Sxb (PFCP)	Session Endpoint ID para comunicação PGW-U
Session-ID	Gx (Diameter)	Sessão Diameter para comunicação PCRF
Charging-ID	Accounting	ID único para cobrança

Dados da Sessão



Criação da Sessão

Fluxo de Chamadas



Etapas

1. Receber Solicitação de Criação de Sessão (S5/S8)

A criação da sessão é iniciada via sinalização GTP-C na interface S5/S8. Veja Interface S5/S8 para detalhes completos do protocolo GTP-C e formatos de mensagem.

Entrada:

- IMSI, MSISDN, IMEI
- APN (por exemplo, "internet")
- Tipo de RAT (EUTRAN)
- Localização do UE (TAI, ECGI)
- Contexto do Bearer (QoS, F-TEID)

2. Alocação de Recursos

```
- Alocar IP do UE do pool de APN
- Gerar ID de Cobrança
- Gerar Gx Session-ID
- Alocar S5/S8 TEID
- Selecionar par PGW-U
```

3. Solicitação de Política (Gx)

Solicitar política ao PCRF:

- Enviar CCR-Initial
- Receber CCA-Initial com QoS e regras PCC

4. Configuração do Plano do Usuário (PFCP)

Programar o PGW-U com regras de encaminhamento:

- Enviar Solicitação de Estabelecimento de Sessão
- Incluir PDRs, FARs, QERs, BAR
- Receber F-TEID para o túnel S5/S8

5. Resposta ao SGW-C

Enviar Resposta de Criação de Sessão:

- Endereço IP do UE
- S5/S8 F-TEID (do PGW-U)
- PCO (DNS, P-CSCF, MTU)
- Contexto do Bearer

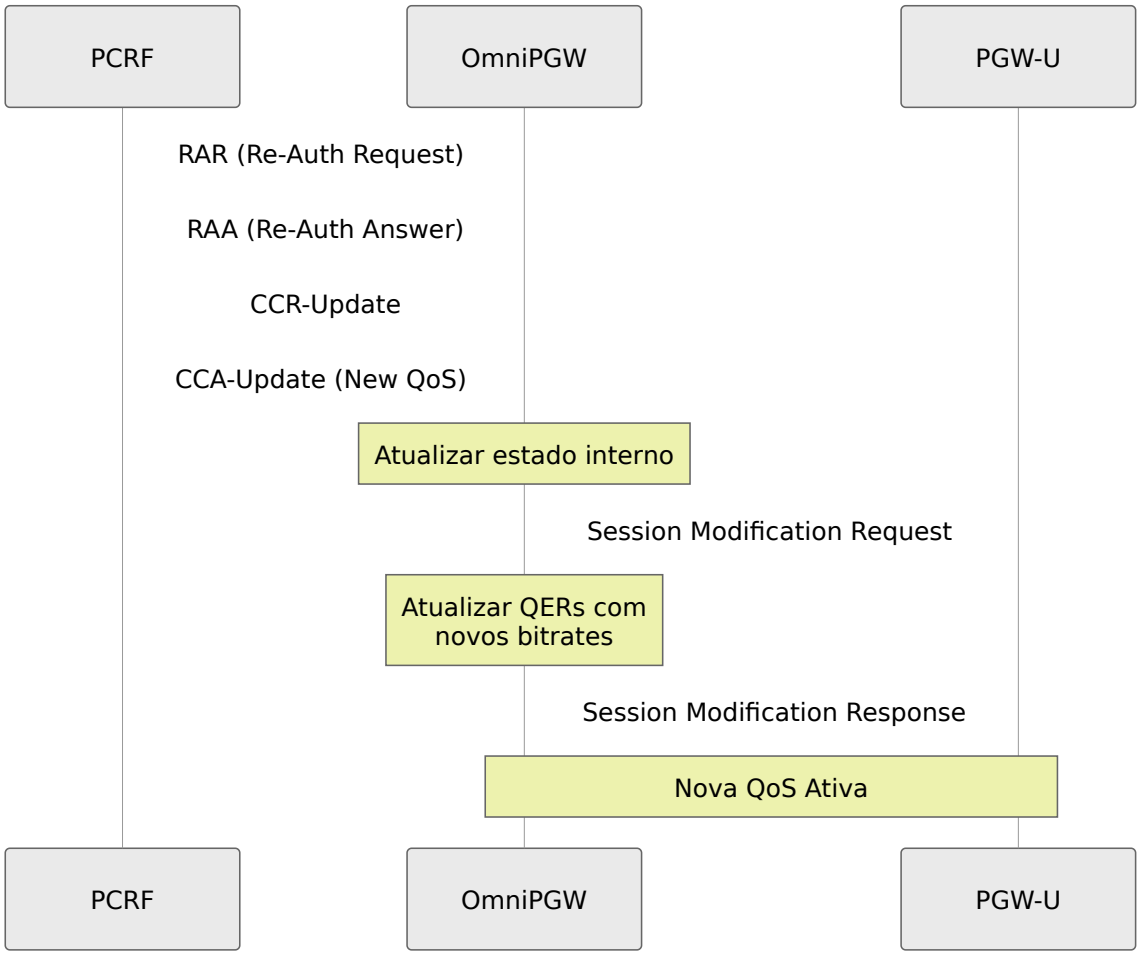
Modificação da Sessão

Gatilhos

As sessões podem ser modificadas devido a:

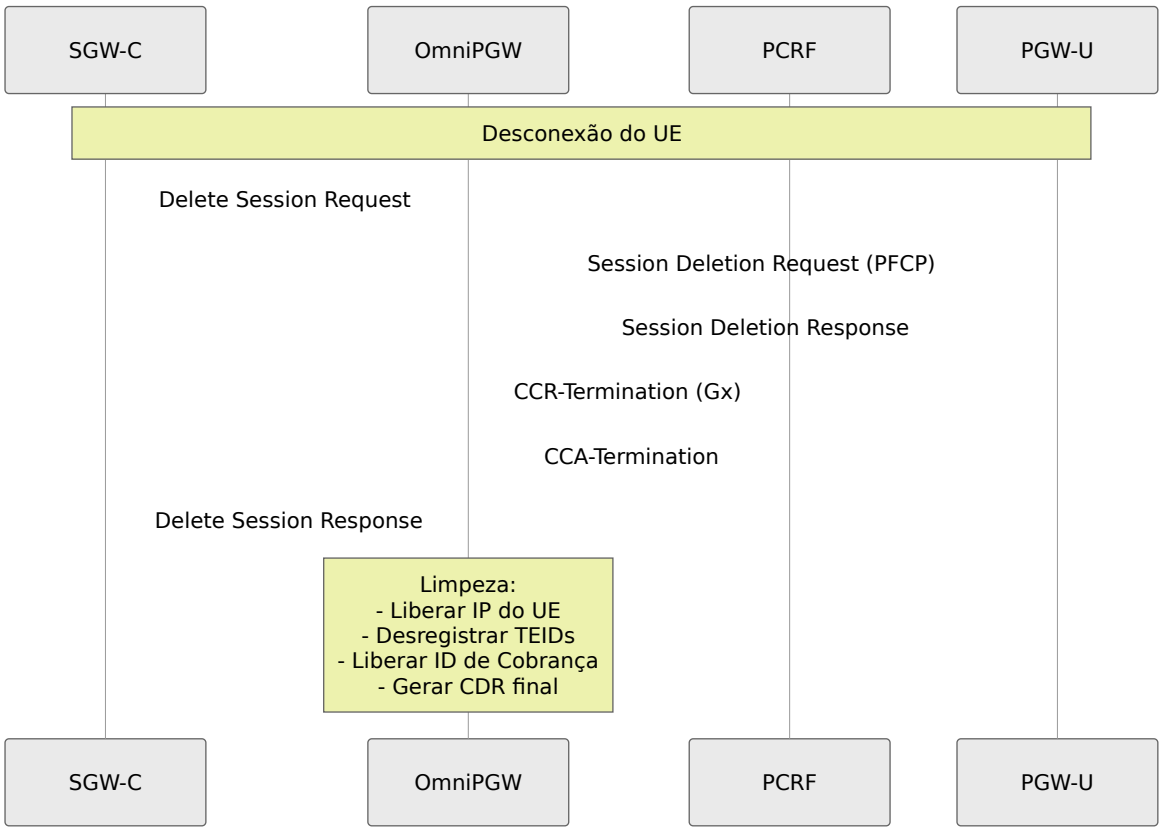
- **Mudanças de QoS** - Atualizações de bitrate pelo PCRF
- **Operações de Bearer** - Adicionar/remover bearers dedicados
- **Handover** - Mudança de SGW
- **Atualizações de Política** - Novas regras PCC do PCRF

Fluxo de Modificação de QoS



Exclusão da Sessão

Fluxo de Chamadas



Processo de Limpeza

Recursos Liberados:

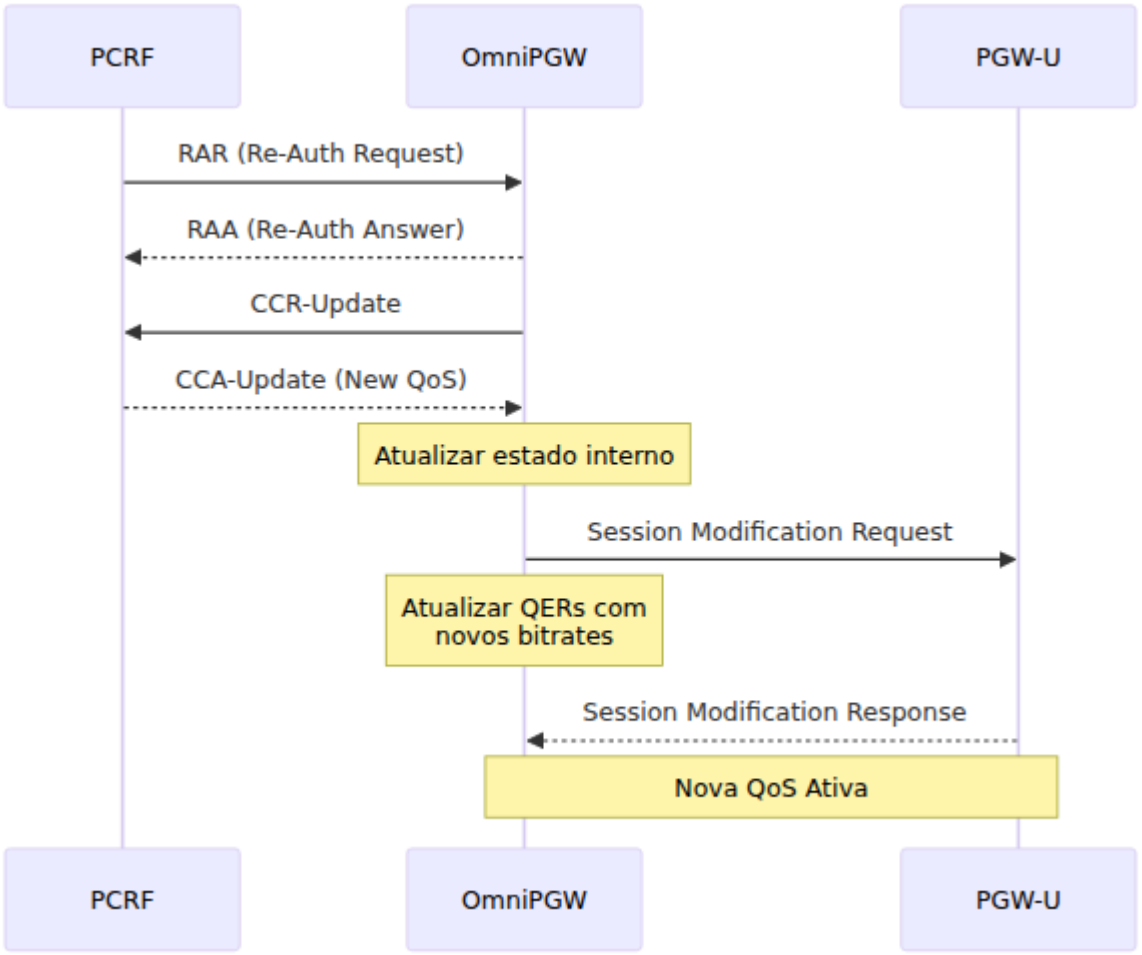
1. Endereço IP do UE → de volta ao pool
2. TEID → removido do registro
3. SEID → removido do registro
4. Session-ID → removido do registro
5. Charging-ID → liberado
6. Processo da sessão encerrado

Registros de Cobrança Gerados:

- CDR final (Charging Data Record) escrito para cobrança offline - Veja Formato de CDR de Dados

Estado da Sessão

Máquina de Estados



Rastreamento da Sessão

Consultas ao Registro:

```
Por TEID (S5/S8):
  TEID 0x12345678 → Session PID

Por SEID (Sxb):
  SEID 0xABCDEF → Session PID

Por Session-ID (Gx):
  "pgw.example.com;123;456" → Session PID

Por IP do UE:
  100.64.1.42 → Session PID

Por IMSI + EBI:
  "310260123456789" + EBI 5 → Session PID
```

Monitoramento de Sessões

Contagem de Sessões Ativas

```
# Total de sessões ativas
teid_registry_count

# Sessões PFCP
seid_registry_count

# Sessões Gx
session_id_registry_count
```

Métricas da Sessão

```
# Taxa de criação de sessões
rate(s5s8_inbound_messages_total{message_type="create_session_request

# Taxa de exclusão de sessões
rate(s5s8_inbound_messages_total{message_type="delete_session_request

# Latência de criação de sessão (p95)
histogram_quantile(0.95,

rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m])
)
```

Problemas Comuns

Falhas na Criação da Sessão

Causas:

1. **Pool de IPs Esgotado** - Nenhum IP disponível
2. **PCRF Inacessível** - Timeout Gx
3. **PGW-U Fora do Ar** - Nenhum par PFCP disponível
4. **Rejeição do PCRF** - Usuário desconhecido, não autorizado

Debug:

```
# Verificar pool de IPs
curl http://pgw:9090/metrics | grep address_registry_count

# Verificar conectividade com o PCRF
# Verificar erros Gx nos logs

# Verificar associação PGW-U
# Verificar status do par PFCP
```

Sessão Travada/Obsoleta

Sintomas:

- Sessão não excluída corretamente
- Recursos não liberados
- Registros mostram contagem maior do que o esperado

Causas:

1. Solicitação de Exclusão de Sessão não recebida
2. Falha do processo da sessão sem limpeza
3. Vazamento de registro

Resolução:

```
# Reiniciar OmniPGW (libera todas as sessões)
# Implementar mecanismo de timeout de sessão
```

UE Não Consegue Estabelecer Sessão

Sintomas:

- Falha na conexão do UE
- Resposta de Criação de Sessão com causa de erro

Causas Comuns e Respostas:

Valor da Causa	Significado	Ação
Usuário Desconhecido	PCRF rejeitou (IMSI não está no banco de dados)	Provisionar assinante
Recursos Não Disponíveis	Pool de IP esgotado	Expandir pool de IP
Par Remoto Não Respondendo	Timeout PCRF/PGW-U	Verificar conectividade
Serviço Não Suportado	APN inválido	Configurar pool de APN

Melhores Práticas

Limites de Sessão

Configurar capacidade apropriada:

```
Usuários concorrentes esperados: 10.000
Sobrecarga de sessão por usuário: ~10KB RAM
RAM total para sessões: ~100MB

Configurações da VM Erlang:
  - Máximo de processos: 262.144 (padrão)
  - Tamanho do heap do processo: Ajustar com base na carga
```

Limpeza de Sessão

Garantir limpeza adequada:

1. Sempre responder a Solicitações de Exclusão de Sessão
2. Implementar timeout de sessão para sessões obsoletas

3. Monitorar contagens de registro para vazamentos

Alta Disponibilidade

Redundância de Sessão:

- Usar design sem estado (sessões vinculadas à instância)
- Implementar banco de dados de sessão para HA (futuro)
- DNS/balanceador de carga para failover

Elementos de Dados da Sessão

Que Informações Uma Sessão Armazena?

Cada sessão PDN ativa mantém as seguintes informações:

Identificação do UE:

- IMSI: "310260123456789" (identidade do assinante)
- MSISDN: "14155551234" (número de telefone)
- MEI/IMEI: Identificador do dispositivo

Detalhes da Conexão PDN:

- APN: "internet" (nome da rede)
- Endereço IP do UE: 100.64.1.42 (IP alocado)
- Tipo de PDN: IPv4, IPv6 ou IPv4v6

Identificadores da Sessão:

- ID de Cobrança: Identificador único de cobrança
- EBI do Bearer Padrão: EPS Bearer Identifier (tipicamente 5)

Parâmetros de QoS:

- APN-AMBR: Taxa Máxima de Bits Agregada

    - Uplink: 100 Mbps
    - Downlink: 50 Mbps

Regras de Encaminhamento:

- PDRs (Regras de Detecção de Pacotes): Combinar pacotes
- FARs (Regras de Ação de Encaminhamento): Ações de encaminhamento/descartes
- QERs (Regras de Aplicação de QoS): Limitação de taxa
- BAR (Regra de Ação de Bufferização): Bufferização de downlink

Contexto da Interface:

- Estado S5/S8: TEIDs locais/remotos, endereço SGW-C
- Estado Sxb: SEIDs locais/remotos, endereço PGW-U
- Estado Gx: Session-ID Diameter, contador de solicitações

UI Web - Monitoramento de Sessões Ao Vivo

O OmniPGW inclui uma **UI Web** em tempo real para monitorar sessões ativas sem precisar consultar métricas ou logs.

Pesquisa de UE & Análise Detalhada

Acesso: `http://<omnipgw-ip>:<web-port>/ue_search`

Propósito: Pesquisar sessões específicas de UE e visualizar informações detalhadas

Recursos:

1. Funcionalidade de Pesquisa Pesquisar sessões por:

- **IMSI** (por exemplo, "310170123456789")
- **MSISDN** (número de telefone)
- **Endereço IP** (por exemplo, "100.64.1.42")

2. Opções de Pesquisa

- Seletor suspenso para escolher o tipo de pesquisa
- Pesquisa em tempo real com resultados instantâneos
- Interface clara com dicas de pesquisa

3. Resultados de Análise Detalhada Uma vez encontrado, exibe informações abrangentes da sessão:

a) Sessões Ativas

- Todas as sessões ativas para este assinante

- IMSI, MSISDN, Endereço IP do UE
- APN, Tipo de RAT
- PGW TEID, SGW TEID

b) Localização Atual Dados de localização em tempo real da sessão:

- **TAC** (Código da Área de Rastreamento) - Área de rastreamento onde o UE está localizado
- **ID da Célula (ECI)** - Identificador da Célula E-UTRAN
- **ECGI** - Identificador Global da Célula E-UTRAN (PLMN + ECI)
- **MCC/MNC** - Código do País Móvel / Código da Rede Móvel

Integração com Banco de Dados de Torres de Celular: Se o banco de dados OpenCellID estiver configurado, a interface exibirá:

- Coordenadas geográficas da torre de celular (latitude/longitude)
- Google Maps incorporado mostrando a localização exata da torre
- Mapa visual do último local conhecido do UE

Veja Configuração do Banco de Dados de Torres de Celular abaixo para instruções de configuração.

c) Informações do Bearer Listagem detalhada do bearer com parâmetros de QoS:

Bearer Padrão:

- EBI (EPS Bearer Identifier)
- QCI (QoS Class Identifier)
- Nome da Regra de Cobrança
- APN-AMBR (uplink/downlink)

Bearers Dedicados (se ativos):

- EBI, QCI, Nome da Regra de Cobrança
- MBR UL/DL (Taxa Máxima de Bits)
- GBR UL/DL (Taxa Garantida de Bits)

d) Informações de Cobrança (Interface Gy)

- ID da Sessão Gy
- Quota Concedida, Quota Usada
- Características de Cobrança

e) Informações de Política (Interface Gx)

- ID da Sessão Gx
- Host de Origem/Destino do PCRF
- Número da Solicitação CC
- Regras de Cobrança Instaladas (regras PCC dos bearers)

f) Eventos Recentes

- Histórico de eventos para este assinante
- Eventos de criação/atualização/exclusão de sessão

Casos de Uso:

- Solucionar problemas específicos de assinantes
- Verificar o estabelecimento da sessão
- Verificar o endereço IP atribuído

- Inspecionar parâmetros da sessão

Página de Sessões do PGW

Acesso: `http://<omnipgw-ip>:<web-port>/pgw_sessions`

Propósito: Visualização em tempo real de todas as sessões PDN ativas

Recursos:

1. Visão Geral da Sessão

- Contagem de sessões ao vivo (atualiza a cada 2 segundos)
- Visualização em grade de todas as sessões ativas
- Sem necessidade de atualização - atualizações automáticas

2. Informações Rápidas da Sessão Visível para cada sessão:

- **IMSI** - Identidade do assinante
- **UE IP** - Endereço IP alocado
- **SGW TEID** - ID do túnel S5/S8 do SGW
- **PGW TEID** - ID do túnel S5/S8 do OmniPGW

- **APN** - Nome do Ponto de Acesso

3. Funcionalidade de Pesquisa Pesquisar sessões por:

- IMSI (por exemplo, "310260")
- Endereço IP do UE (por exemplo, "100.64")
- MSISDN / número de telefone
- Nome da APN

4. Detalhes Expansíveis Clique em qualquer linha de sessão para ver detalhes completos:

- Informações completas do assinante (IMSI, MSISDN, IMEI)
- Contexto da rede (tipo de RAT, MCC/MNC da rede de atendimento)
- Parâmetros de QoS (AMBR uplink/downlink em formato legível)
- Identificadores de túnel (ambos TEIDs em formato hexadecimal)
- ID do processo para depuração
- Estado completo da sessão (estrutura de dados bruta)

Visualização da Topologia da Rede

Acesso: `http://<omnipgw-ip>:<web-port>/topology`

Propósito: Representação visual das conexões de rede e sessões ativas

Recursos:

1. Visualização da Topologia

- Gráfico visual dos elementos da rede
- Mostra o nó PGW-C (Plano de Controle)
- Peers HSS (Home Subscriber Server) conectados
- Exibição da contagem de sessões ativas

2. Elementos Interativos

- Controles de zoom (+/-)
- Botão de centralização da visualização
- Clique nos nós para detalhes
- Mostra o status da conexão (verde = ativo, vermelho = fora do ar)

3. Contagem de Sessões

- Contador de sessões ativas em tempo real
- Atualiza automaticamente
- Indicação visual da carga

Casos de Uso:

- Compreender a arquitetura da rede de relance
- Verificar conexões de peers
- Monitorar mudanças na topologia
- Verificação rápida da saúde da rede

Histórico de Sessões & Log de Auditoria

Acesso: `http://<omnipgw-ip>:<web-port>/session_history`

Propósito: Rastrear eventos históricos de sessão e trilha de auditoria

Recursos:

1. Filtragem de Eventos

- Filtrar por tipo de evento (Todos os Eventos, Sessão Criada, Sessão Excluída, etc.)
- Seleção de intervalo de datas (De Data / Para Data)
- Pesquisar por IMSI, MSISDN, endereço IP ou TEID

2. Funcionalidade de Exportação

- Exportar para CSV para análise
- Inclui todos os resultados filtrados
- Útil para conformidade e relatórios

3. Tipos de Eventos Rastreáveis

- Eventos de criação de sessão
- Eventos de exclusão de sessão
- Eventos de modificação
- Eventos de erro

Casos de Uso:

- Trilhas de auditoria para conformidade
- Análise histórica de sessões
- Solucionar problemas de eventos passados
- Gerar relatórios de uso
- Rastrear padrões de sessão ao longo do tempo

Casos de Uso Operacionais

Verificação da Sessão:

```
1. Usuário relata problema de conectividade
2. Pesquisar UI Web por IMSI ou número de telefone
3. Verificar se a sessão existe e se o UE tem endereço IP
4. Verificar se os valores de QoS correspondem ao plano do
assinante
5. Verificar se os endpoints do túnel estão estabelecidos
```

Monitoramento de Capacidade:

- Olhar para a contagem de sessões ativas
- Comparar com a capacidade licenciada
- Identificar padrões de uso por APN

Solução de Problemas:

- Encontrar sessão específica por qualquer identificador
- Inspecionar estado completo da sessão sem SSH/IEx
- Verificar se os TEIDs do SGW e PGW correspondem entre os sistemas
- Verificar valores de AMBR aplicados do PCRF

Vantagens Sobre Métricas:

- Ver detalhes de sessão individuais (métricas mostram agregados)
- Capacidades de pesquisa e filtragem
- Formatação legível (largura de banda em Mbps, não bps)
- Inspeção de estado em tempo real
- Sem necessidade de acesso à linha de comando

Configuração do Banco de Dados de Torres de Celular

O OmniPGW pode se integrar ao banco de dados OpenCellID para exibir localizações de torres de celular na interface de Pesquisa de UE. Este recurso permite a visualização geográfica de onde os assinantes estão localizados com base em seu site de célula de atendimento.

Visão Geral

Quando configurado, a interface de Pesquisa de UE irá:

- Exibir coordenadas da torre de celular (latitude/longitude)
- Mostrar uma visualização do Google Maps incorporada da localização da torre
- Fornecer confirmação visual da localização do assinante
- Ajudar a solucionar problemas de roteamento baseados em localização

Configuração

Acesse a página de Torres de Celular em `http://<omnipgw-ip>:<web-port>/cell_towers` e clique no botão **"Redownload Database"**. Isso aciona um processo automático de download e importação em segundo plano.

Recursos:

- Baixa dados frescos do OpenCellID.org
- Extrai e importa automaticamente para SQLite
- Executa em segundo plano (leva de 10 a 15 minutos)
- Mostra notificações de progresso via interface web
- Seguro: só exclui o banco de dados antigo após confirmar que o novo download foi bem-sucedido

Configuração Inicial: Quando você acessar pela primeira vez a página de Torres de Celular, ela mostrará instruções de configuração com o botão "Redownload Database". Basta clicar nele para inicializar o banco de dados.

Informações do Banco de Dados

Localização do Banco de Dados:

- DB SQLite: `priv/cell_towers.db`
- Download CSV (temporário): `priv/data/cell_towers.csv.gz`
- Índices: Criados automaticamente em MCC, MNC, LAC, CellID para buscas rápidas

Tamanho do Banco de Dados:

- ~107 MB de download comprimido do OpenCellID.org
- Tempo de importação: 10-15 minutos dependendo do hardware

Desempenho da Consulta:

- Consultas de torres de celular são indexadas e muito rápidas (<1ms)
- Sem impacto no desempenho do estabelecimento da sessão
- Consultas ocorrem apenas ao visualizar resultados da Pesquisa de UE

Recursos Habilitados

Após a configuração, os seguintes recursos ficam disponíveis:

Página de Pesquisa de UE:

- Seção de Localização Atual mostra coordenadas da torre de celular
- Google Maps incorporado exibindo localização da torre
- Representação visual do último site de célula conhecido do assinante

UI Web de Torres de Celular:

- Ver estatísticas do banco de dados (total de registros, tamanho do banco de dados, data de criação)
- **Botão Redownload Database** - Atualização com um clique para os dados mais recentes do OpenCellID
- Navegar pelo banco de dados de torres de celular
- Pesquisar por MCC, MNC, LAC, Cell ID
- Ver distribuição geográfica das torres
- Ver instruções de configuração se o banco de dados ainda não estiver configurado

Benefícios Operacionais:

- Identificar rapidamente a localização geográfica do assinante
- Verificar cenários de roaming
- Solucionar problemas baseados em localização
- Apoiar requisitos de localização de serviços de emergência

Atualizando o Banco de Dados

O banco de dados OpenCellID é mantido pela comunidade e atualizado regularmente.

Para atualizar seu banco de dados local:

1. Navegue até `http://<omnipgw-ip>:<web-port>/cell_towers`
2. Clique no botão **"Redownload Database"**

3. Confirme a ação na caixa de diálogo pop-up
4. Aguarde de 10 a 15 minutos para que o download/importação em segundo plano seja concluído
5. Atualize a página para ver as estatísticas atualizadas

Frequência de Atualização Recomendada: Mensal ou trimestral

Nota: O OpenCellID pode limitar a taxa de downloads. Se você fez o download recentemente, aguarde algumas horas antes de tentar novamente.

Solução de Problemas

Falhas no Redownload:

- Verifique a conectividade com a internet para OpenCellID.org
- Verifique se o firewall permite downloads HTTPS
- Verifique o espaço em disco (~200 MB de espaço livre requerido)
- Verifique os logs da aplicação para mensagens de erro específicas
- O OpenCellID pode estar limitando a taxa - aguarde algumas horas e tente novamente
- Verifique se a UI web mostra a mensagem de erro da tarefa em segundo plano

Erros de Gravação no Banco de Dados:

- Verifique as permissões de gravação do banco de dados no diretório `priv/`
- Certifique-se de que há espaço em disco suficiente (~150 MB para o banco de dados)
- Verifique se a aplicação tem permissão para criar/excluir arquivos em `priv/`

Torre de Celular Não Encontrada:

- O banco de dados pode não ter cobertura para todos os sites de células
- O OpenCellID é contribuído pela comunidade e pode ter lacunas
- Os dados da torre de celular podem estar desatualizados para sites recém-implantados

Mapa Não Exibindo:

- Verifique o console JavaScript do navegador para erros
- Verifique as permissões de incorporação do Google Maps
- Verifique se as coordenadas da torre de celular são válidas

---

Documentação Relacionada

Funções Centrais da Sessão

- **Interface PFCP** - Estabelecimento de sessão do plano do usuário, PDRs, FARs, QERs, URRs
- **Alocação de IP do UE** - Atribuição de endereço IP, gerenciamento do pool de APN
- **Configuração do PCO** - Parâmetros DNS, P-CSCF, MTU entregues ao UE
- **Guia de Configuração** - Seleção de UPF, fluxos de estabelecimento de sessão

Política e Cobrança

- **Interface Diameter Gx** - Controle de política PCRF, regras PCC, gerenciamento de QoS
- **Interface Diameter Gy** - Cobrança online OCS, rastreamento de quota
- **Formato de CDR de Dados** - Geração de registros de cobrança offline

Interfaces de Rede

- **Interface S5/S8** - Protocolo GTP-C, comunicação SGW-C
- **Gerenciamento de QoS e Bearer** - Aplicação de QoS do bearer

Operações

- **Guia de Monitoramento** - Métricas de sessão, rastreamento de sessões ativas, alertas

- **Monitoramento P-CSCF** - Monitoramento de sessão IMS

Voltar ao Guia de Operações

Gerenciamento de Sessão OmniPGW - *por Omnitouch Network Services*

Guia de Solução de Problemas do OmniPGW

Procedimentos de Solução de Problemas e Problemas Comuns

por Omnitouch Network Services

Índice

Visão Geral

Este guia fornece procedimentos de solução de problemas passo a passo para problemas operacionais comuns do OmniPGW. Cada problema inclui:

- **Sintoma**: O que você observará
- **Causas Prováveis**: Causas raiz comuns
- **Diagnóstico**: Como confirmar a causa
- **Resolução**: Correção passo a passo
- **Prevenção**: Como evitar recorrências

Documentação Relacionada

- **Guia de Monitoramento** - Métricas do Prometheus, alertas, monitoramento de desempenho
- **Guia de Configuração** - Referência de configuração do sistema

---

Ferramentas de Solução de Problemas

Interface Web

Acesso: `http://<omnipgw_ip>:4000`

Páginas Principais:

- **/pgw_sessions** - Visualizador de sessões em tempo real (pesquisar por IMSI, IP, MSISDN, APN)
- **/diameter** - Status do par de Diâmetro (Gx PCRF, Gy OCS)
- **/pfcp_peers** - Status do par de PFCP (conectividade PGW-U)
- **/logs** - Streaming de logs em tempo real com filtragem

Métricas do Prometheus

Acesso: `http://<omnipgw_ip>:9090/metrics`

Métricas Principais:

- `teid_registry_count` - Sessões ativas
- `address_registry_count` - IPs de UE alocados
- `sxb_inbound_errors_total` - Erros de PFCP
- `gx_inbound_errors_total` - Erros de Diâmetro Gx
- `gy_inbound_errors_total` - Erros de Diâmetro Gy

Veja o Guia de Monitoramento para referência completa de métricas.

Análise de Logs

Interface Web: Acesse a página **/logs** e use filtros de pesquisa

Filtros Comuns de Log:

- "create_session_request" - Estabelecimento de sessão
- "Credit Control" - Interações Gx/Gy
- "PFCP Session" - Programação do plano do usuário
- "error" ou "ERROR" - Mensagens de erro
- "timeout" - Problemas de timeout

Problemas de Estabelecimento de Sessão

Problema: Solicitação de Criação de Sess��o Rejeitada com "Nenhum Recurso Disponível"

Sintoma:

- SGW-C recebe Resposta de Criação de Sessão com causa "Nenhum recurso disponível" (73)
- Todas as tentativas de nova sessão falham
- Sessões existentes continuam funcionando
- Logs: `[PGW-C] Solicitação de Criação de Sessão bloqueada - licença inválida`

Captura do Wireshark mostrando Resposta de Criação de Sessão com causa "Nenhum recurso disponível"

Causa Provável:

- Licença do OmniPGW inválida ou expirada
- Servidor de licença inacessível

Diagnóstico:

1. **Verifique a métrica da licença:**

   ```
   license_status
   ```

   - Valor de 0 indica licença inválida
2. **Verifique os logs em busca de avisos de licença:**
   - Pesquisar por "license" ou "License"
   - Procure por mensagens "Unable to contact license server"
3. **Verifique a conectividade do servidor de licença:**
   - Verifique a URL configurada em `config/runtime.exs` sob `:license_client`

- Padrão: `https://localhost:10443/api`

Resolução:

1. **Verifique se o servidor de licença é acessível:**

```
curl -k https://<license_server_ip>:10443/api/status
```

2. **Verifique a configuração da licença em `config/runtime.exs`:**

```
config :license_client,
  license_server_api_urls:
["https://<license_server_ip>:10443/api"],
  licensee: "Seu Nome da Empresa"
```

3. **Verifique se o produto está licenciado:**
   - Nome do produto: `omnipgwc`
   - Entre em contato com a Omnitouch para verificar o status da licença
4. **Reinicie o OmniPGW após alterações de configuração**

Prevenção:

- Monitore a métrica `license_status` com alertas críticos
- Assegure alta disponibilidade do servidor de licença
- Configure alertas de expiração de licença antes da expiração

---

Problema: Solicitação de Criação de Sessão Rejeitada (Outras Causas)

Sintoma:

- SGW-C recebe Resposta de Criação de Sessão com causa de erro
- Usuários não conseguem estabelecer conexões PDN
- Métrica: `s5s8_inbound_errors_total` aumentando

Causas Prováveis:

1. Pool de IP esgotado
2. PCRF (Gx) inacessível ou rejeitando política
3. PGW-U (PFCP) indisponível
4. Configuração de APN inválida

Diagnóstico:

1. **Verifique a utilização do pool de IP:**

   ```
   address_registry_count
   ```

   - Se igual ao tamanho do pool configurado, o pool está esgotado

2. **Verifique a conectividade do PCRF:**

   - Interface Web → página **/diameter**
   - Procure por status do par PCRF = "desconectado"
   - Logs: Pesquisar "Credit Control Answer" por erros

3. **Verifique o status do par PFCP:**

   - Interface Web → página **/pfcp_peers**
   - Procure por "Association: DOWN"
   - Métrica: `pfcp_peer_associated` = 0

4. **Verifique a configuração de APN:**

   - Revise `config/runtime.exs` sob `ue.apn_map`
   - Verifique se a APN solicitada existe na configuração

Resolução:

Para Esgotamento do Pool de IP:

1. Identifique sessões obsoletas: Interface Web → **/pgw_sessions**, procure por sessões antigas
2. Expanda o pool de IP em `config/runtime.exs`:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => "10.0.0.0/23"  # Alterado de /24 para /23
(dobra a capacidade)
    }
  }
```

3. Reinicie o OmniPGW
4. Verifique: `curl http://<ip>:9090/metrics | grep address_registry_count`

Para Problemas de Conectividade do PCRF:

1. Verifique a conectividade da rede: `ping <pcrf_ip>`
2. Verifique o serviço de Diâmetro do PCRF: `telnet <pcrf_ip> 3868`
3. Verifique a configuração do par de Diâmetro em `config/runtime.exs`
4. Reinicie o OmniPGW se a configuração foi alterada
5. Verifique via Interface Web → **/diameter** (o par deve mostrar "conectado")

Para Problemas de PFCP:

- Veja a seção Problemas de PFCP / Plano do Usuário

Prevenção:

- Monitore a utilização do pool de IP com alertas em 80%
- Monitore a conectividade do PCRF com alertas de par de Diâmetro
- Implemente limpeza de sessões para sessões ociosas

Problema: Sessões Presas em Estado Intermediário

Sintoma:

- A sessão aparece na Interface Web, mas incompleta

- Métricas mostram contagem crescente de sessões, mas sem tráfego de usuários
- Solicitação de Exclusão de Sessão falha ou expira

Causas Prováveis:

1. Estabelecimento de Sessão PFCP falhou, mas sessão S5/S8 criada
2. CCR-Initial do PCRF expirou
3. Solicitação de Criação de Bearer (bearer dedicado) falhou
4. Interrupção da rede durante a configuração da sessão

Diagnóstico:

1. **Pesquise a sessão na Interface Web:**
    - **/pgw_sessions** → Pesquisar por IMSI
    - Verifique se `pfcp_seid` está presente (se ausente, PFCP falhou)
    - Verifique se `gx_session_id` está presente (se ausente, Gx falhou)
2. **Verifique os logs para o IMSI:**
    - Filtrar logs por IMSI
    - Procure por "Solicitação de Estabelecimento de Sessão" (PFCP)
    - Procure por "Solicitação de Controle de Crédito" (Gx)
    - Procure por mensagens de timeout ou erro
3. **Verifique as métricas:**

```
# Sessões com TEID, mas sem sessão PFCP
teid_registry_count - seid_registry_count

# Sessões com TEID, mas sem sessão Gx
teid_registry_count - session_id_registry_count
```

Resolução:

1. **Para falhas de estabelecimento PFCP:**
    - Verifique a saúde e os logs do PGW-U

- Verifique a associação PFCP: Interface Web → **/pfcp_peers**
- Envie Solicitação de Exclusão de Sessão do SGW-C para limpeza

2. **Para problemas de timeout Gx:**
   - Verifique a latência do PCRF: `histogram_quantile(0.95, rate(gx_outbound_transaction_duration_bucket[5m]))`
   - Aumente o timeout Gx em `config/runtime.exs` se necessário
   - Envie Solicitação de Exclusão de Sessão para limpeza
3. **Limpeza manual (último recurso):**
   - Atualmente requer reinício do OmniPGW para limpar sessões presas
   - Monitore `teid_registry_count` antes/depois do reinício para confirmar limpeza

Prevenção:

- Monitore as métricas de latência PFCP e Gx
- Implemente timeout/limpeza de sessão para sessões incompletas
- Alerta sobre discrepâncias na contagem do registro

Problemas de PFCP / Plano do Usuário

Problema: Associação PFCP Desconectada

Sintoma:

- Interface Web → **/pfcp_peers** mostra "Associação: DOWN"
- Todas as novas estabelecimentos de sessão falham
- Métrica: `pfcp_peer_associated` = 0
- Logs: "Timeout de heartbeat PFCP" ou "Falha na configuração da associação"

Causas Prováveis:

1. PGW-U inacessível (problema de rede)
2. PGW-U travou ou reiniciou
3. Incompatibilidade de configuração de PFCP (IP, porta)
4. Firewall bloqueando UDP 8805

Diagnóstico:

1. **Verifique a conectividade da rede:**

```
ping <pgw_u_ip>
nc -u -v <pgw_u_ip> 8805
```

2. **Verifique a configuração de PFCP:**
   - Revise `config/runtime.exs` sob `upf.peer_list`
   - Verifique se o endereço IP e o ID do nó correspondem à configuração do PGW-U
3. **Verifique o status do PGW-U:**
   - Acesse os logs do PGW-U
   - Verifique se o PGW-U está em execução: `systemctl status omnipgw_u` (ou equivalente)
4. **Verifique as métricas:**

```
# Falhas de heartbeat
pfcp_consecutive_heartbeat_failures

# Taxa de erro de PFCP
rate(sxb_inbound_errors_total[5m])
```

Resolução:

1. **Para problemas de rede:**
   - Verifique o roteamento: `traceroute <pgw_u_ip>`
   - Verifique as regras do firewall: Assegure que UDP 8805 esteja permitido

- Verifique grupos de segurança (se implantação em nuvem)

2. **Para travamentos do PGW-U:**
   - Reinicie o serviço PGW-U
   - Aguarde 30 segundos para reestabelecimento da associação
   - Verifique via Interface Web → **/pfcp_peers** (deve mostrar "Associação: UP")
3. **Para problemas de configuração:**
   - Corrija a configuração do par PFCP em `config/runtime.exs`
   - Reinicie o OmniPGW
   - Verifique se a associação foi estabelecida

Prevenção:

- Monitore a métrica `pfcp_peer_associated` com alertas críticos
- Monitore `pfcp_consecutive_heartbeat_failures` (alerta em > 2)
- Implemente instâncias redundantes do PGW-U
- Habilite keepalive/heartbeat de PFCP (deve ser padrão)

Problema: Falhas na Modificação da Sessão PFCP

Sintoma:

- Criação de bearer dedicado falha
- Atualizações de política de QoS (do RAR do PCRF) falham
- Logs: "Solicitação de Modificação de Sessão falhou"
- Métrica: `sxb_inbound_errors_total{message_type="session_modification_response"}` aumentando

Causas Prováveis:

1. Regras PFCP inválidas (referências PDR/FAR/QER)

2. Esgotamento de recursos do PGW-U
3. Conflitos de ID de regra
4. Bug de software do PGW-U

Diagnóstico:

1. **Verifique os logs:**
    - Filtrar por "Modificação de Sessão" e SEID
    - Procure por códigos de causa de erro na resposta PFCP
    - Causas comuns: "ID de Regra já existe", "Fora de recursos"
2. **Verifique os logs do PGW-U:**
    - Procure por erros de processamento de PFCP
    - Verifique a utilização de recursos (CPU, memória)
3. **Verifique o estado da sessão na Interface Web:**
    - **/pgw_sessions** → Encontre a sessão por IMSI
    - Revise `pdr_map`, `far_map`, `qer_map` em busca de conflitos
    - Procure por IDs duplicados

Resolução:

1. **Para conflitos de regra:**
    - Exclua e recrie o bearer dedicado
    - Se persistir, exclua a sessão e faça o UE reconectar
2. **Para problemas de recursos do PGW-U:**
    - Verifique a capacidade do PGW-U (sessões, PDRs, throughput)
    - Escale o PGW-U se necessário
    - Reduza a carga de sessão na instância afetada do PGW-U
3. **Para bugs de software:**
    - Capture o estado completo da sessão (detalhes da sessão na Interface Web)

- Capture logs de mensagens PFCP
- Relate ao fornecedor com etapas de reprodução

Prevenção:

- Monitore a utilização de recursos do PGW-U
- Teste a criação de bearer dedicado em staging
- Monitore `sxb_inbound_errors_total` com alertas

Problemas de Diâmetro (Gx/Gy)

Problema: Par PCRF Desconectado (Gx)

Sintoma:

- Interface Web → **/diameter** mostra par PCRF "desconectado"
- Sessões criadas sem políticas de QoS (QCI=5 padrão aplicado)
- Logs: "Falha na conexão do par de Diâmetro" ou "Timeout CER/CEA"

Causas Prováveis:

1. PCRF inacessível (problema de rede)
2. Serviço PCRF fora do ar
3. Incompatibilidade de configuração de Diâmetro (Origin-Host, Realm)
4. Firewall bloqueando TCP 3868

Diagnóstico:

1. **Verifique a conectividade da rede:**

```
ping <pcrf_ip>
telnet <pcrf_ip> 3868
```

2. **Verifique a configuração de Diâmetro:**

   - Revise `config/runtime.exs` sob `diameter.peer_list`

- Verifique se `host`, `realm`, `ip` correspondem à configuração do PCRF
- Verifique se `origin_host` corresponde ao que o PCRF espera

3. **Verifique os logs do PCRF:**
   - Procure por CER (Capabilities-Exchange-Request) do PGW-C
   - Procure por razões de rejeição
4. **Verifique as métricas:**

```
# Erros de conexão de Diâmetro
diameter_peer_connected{peer="<pcrf_host>"}
```

Resolução:

1. **Para problemas de rede:**
   - Verifique o roteamento para o PCRF
   - Verifique as regras do firewall: Assegure que TCP 3868 esteja permitido
   - Teste a conectividade: `nc -v <pcrf_ip> 3868`
2. **Para serviço PCRF fora do ar:**
   - Reinicie o serviço PCRF
   - Aguarde a reconexão automática (intervalo de 30s de tentativa)
   - Verifique via Interface Web → **/diameter**
3. **Para incompatibilidade de configuração:**
   - Corrija a configuração de Diâmetro em `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    host: "pgw-c.epc.mnc999.mcc999.3gppnetwork.org",  #
Deve corresponder à configuração do PCRF
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "192.168.1.100",
        initiate_connection: true
      }
    ]
  }
```

- Reinicie o OmniPGW
- Verifique se a conexão foi estabelecida

Prevenção:

- Monitore a conectividade do par de Diâmetro com alertas críticos
- Implemente instâncias redundantes do PCRF (se suportado)
- Documente a configuração de Diâmetro no runbook

Problema: Timeouts de CCR/CCA (Solicitações de Política Gx)

Sintoma:

- Estabelecimento de sessão lento (> 5 segundos)
- Logs: "Timeout de Solicitação de Controle de Crédito"
- Métrica: `gx_outbound_transaction_duration` muito alta (> 5s)
- Sessões criadas com QoS padrão (comportamento de fallback)

Causas Prováveis:

1. PCRF sobrecarregado
2. Banco de dados do PCRF lento

3. Latência de rede
4. Problema de software do PCRF

Diagnóstico:

1. **Verifique a latência Gx:**

```
# Latência P95
histogram_quantile(0.95,
rate(gx_outbound_transaction_duration_bucket[5m]))

# Latência P99 (outliers)
histogram_quantile(0.99,
rate(gx_outbound_transaction_duration_bucket[5m]))
```

2. **Verifique a saúde do PCRF:**
   - Acesse dashboards de monitoramento do PCRF
   - Verifique CPU, memória, conexões de banco de dados
   - Revise os logs do PCRF em busca de consultas lentas
3. **Verifique a latência da rede:**

```
ping -c 100 <pcrf_ip> | tail -1  # Verifique a latência média
```

4. **Verifique os logs:**
   - Conte as trocas CCR/CCA: Filtrar "Credit Control"
   - Meça o tempo entre "Enviando CCR" e "Recebido CCA"

Resolução:

1. **Para sobrecarga do PCRF:**
   - Escale o PCRF (adicione instâncias)
   - Reduza o tamanho da mensagem CCR, se possível
   - Ajuste pools de threads/trabalhadores do PCRF
2. **Para latência de rede:**

- Investigue o caminho da rede (roteadores, switches)
- Considere co-localizar PGW-C e PCRF

3. **Solução temporária (aumentar timeout):**
   - Edite `config/runtime.exs`:

```
config :pgw_c,
  diameter: %{
    transaction_timeout_ms: 10000  # Aumentar de 5000 para
10000
  }
```

   - Reinicie o OmniPGW
   - **Nota:** Isso apenas mascara o problema; corrija a causa raiz

Prevenção:

- Monitore a latência Gx com alertas (aviso > 1s, crítico > 5s)
- Planeje a capacidade do PCRF para a taxa de sessão esperada
- Teste o desempenho do PCRF sob carga

Problema: Par OCS Desconectado (Gy)

Sintoma:

- Interface Web → **/diameter** mostra par OCS "desconectado"
- Sessões não podem ser cobradas (cobrança online falha)
- Logs: "Falha na conexão do par Gy"

Diagnóstico e Resolução:

Semelhante ao Par PCRF Desconectado, mas para a interface Gy.

Principais diferenças:

- Porta: Normalmente TCP 3868 (mesma do Gx)

- Impacto: Cobrança falha, sessões podem ser rejeitadas ou permitidas sem cobrança (depende da configuração)
- Configuração: Verifique `diameter.peer_list` para a entrada OCS

Veja: Interface Gy de Diâmetro para solução de problemas específicos de Gy

---

Problemas de Alocação de IP

Problema: Pool de IP Esgotado

Sintoma:

- Solicitação de Criação de Sessão rejeitada com causa "Nenhum recurso disponível"
- Métrica: `address_registry_count` igual ao tamanho do pool configurado
- Interface Web → **/pgw_sessions** mostra muitas sessões ativas
- Logs: "Falha na alocação de IP: pool esgotado"

Causas Prováveis:

1. Pool muito pequeno para a base de assinantes
2. Sessões não liberando IPs (falhas de Exclusão de Sessão)
3. Rotatividade rápida de sessões sem limpeza
4. Vazamento de endereço IP

Diagnóstico:

1. **Verifique a utilização do pool:**

```
# Para sub-rede /24 (254 IPs)
(address_registry_count / 254) * 100
```

2. **Verifique o tamanho do pool configurado:**
    - Revise `config/runtime.exs` sob `ue.subnet_map`

- Exemplo: "10.0.0.0/24" = 254 IPs utilizáveis

3. **Compare a contagem de sessões com a contagem de IPs:**

```
# Deve ser aproximadamente igual
teid_registry_count
address_registry_count
```

4. **Revise as sessões ativas:**

- Interface Web → **/pgw_sessions**
- Classifique por hora de início da sessão
- Procure por sessões muito antigas (potenciais vazamentos)

Resolução:

Imediata (expandir pool):

1. Edite `config/runtime.exs`:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => "10.0.0.0/22"  # 1022 IPs (era /24 = 254
IPs)
    }
  }
```

2. Reinicie o OmniPGW
3. Verifique: Sessões agora podem ser estabelecidas

A longo prazo (limpeza):

1. Identifique sessões obsoletas na Interface Web
2. Coordene com SGW-C para enviar Solicitações de Exclusão de Sessão
3. Implemente política de timeout de sessão no PCRF/SGW
4. Monitore `address_registry_count` para verificar se o pool foi liberado após a limpeza

Prevenção:

- Monitore a utilização do pool de IP com alertas:
  - Aviso: > 70%
  - Crítico: > 85%
- Análise de tendência para prever esgotamento
- Implemente timeout de inatividade de sessão
- Auditorias regulares de sessão

Problema: Endereço IP Duplicado Atribuído

Sintoma:

- UE relata conflito de endereço IP
- Logs: aviso "IP já alocado"
- Duas sessões na Interface Web com o mesmo endereço IP

Causas Prováveis:

1. Bug de software (raro)
2. Inconsistência de banco de dados após falha
3. Erro de intervenção manual

Diagnóstico:

1. **Pesquise o IP na Interface Web:**
   - **/pgw_sessions** → Pesquisar por endereço IP
   - Verifique se múltiplos IMSIs têm o mesmo IP
2. **Verifique os logs:**
   - Pesquisar pelo endereço IP
   - Procure por eventos de "alocação de IP"

Resolução:

1. **Identifique as sessões afetadas:**
   - Anote ambos os IMSIs com IP duplicado

2. **Exclua uma sessão:**
    - Coordene com SGW-C para enviar Solicitação de Exclusão de Sessão para um IMSI
    - Prefira excluir a sessão mais nova
3. **UE reconecta:**
    - O UE deve reconectar automaticamente
    - Receberá um novo IP único
4. **Se persistir:**
    - Reinicie o OmniPGW para reconstruir o registro de IP
    - Todas as sessões serão perdidas (coordene a janela de manutenção)

Prevenção:

- Monitore alocações duplicadas (nenhuma métrica interna atualmente)
- Verificações regulares de integridade do banco de dados (se aplicável)

Referência Rápida

Consultas Comuns do Prometheus

```
# Sessões ativas
teid_registry_count

# Taxa de configuração de sessão (por segundo)
rate(s5s8_inbound_messages_total{message_type="create_session_request

# Utilização do pool de IP (para sub-rede /24)
(address_registry_count / 254) * 100

# Latência de configuração de sessão P95
histogram_quantile(0.95,
rate(s5s8_inbound_handling_duration_bucket{request_message_type="crea
[5m]))

# Taxa de erro
rate(s5s8_inbound_errors_total[5m])

# Latência do PCRF
histogram_quantile(0.95, rate(gx_outbound_transaction_duration_bucket

# Status da associação PFCP
pfcp_peer_associated
```

Filtros Comuns de Log (Interface Web)

Filtro	Propósito
IMSI	Encontrar todos os logs para assinante específico
"create_session"	Fluxo de estabelecimento de sessão
"delete_session"	Fluxo de encerramento de sessão
"Credit Control"	Interações Gx PCRF
"PFCP Session"	Programação do plano do usuário
"error"	Todas as mensagens de erro
"timeout"	Problemas de timeout
"Association"	Eventos de associação PFCP

Comandos de Verificação de Saúde

```
# Verifique o status do serviço
systemctl status omnipgw_c

# Verifique a interface web
curl http://<omnipgw_ip>:4000

# Verifique o endpoint de métricas
curl http://<omnipgw_ip>:9090/metrics

# Verifique sessões ativas
curl http://<omnipgw_ip>:9090/metrics | grep teid_registry_count

# Verifique a associação PFCP
curl http://<omnipgw_ip>:9090/metrics | grep pfcp_peer_associated

# Verifique a utilização do pool de IP
curl http://<omnipgw_ip>:9090/metrics | grep
address_registry_count
```

Documentação Relacionada

- **Guia de Monitoramento** - Métricas do Prometheus, dashboards do Grafana, alertas
- **Guia de Configuração** - Referência de configuração do sistema
- **Gerenciamento de Sessão** - Detalhes do ciclo de vida da sessão
- **Interface PFCP** - Detalhes de solução de problemas de PFCP
- **Interface Gx de Diâmetro** - Solução de problemas de política Gx
- **Interface Gy de Diâmetro** - Solução de problemas de cobrança Gy
- **QoS & Gerenciamento de Bearer** - Problemas relacionados a QoS

Voltar ao Guia de Operações

Guia de Solução de Problemas do OmniPGW - *por Omnitouch Network Services*

Documentação de Alocação de Pool de IP da UE

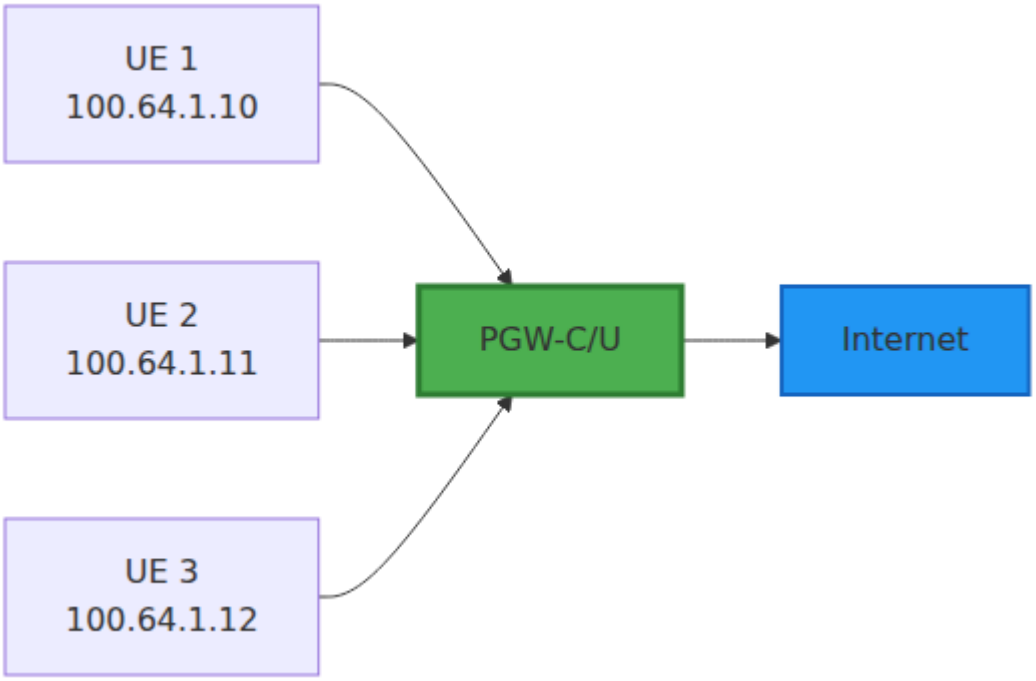
Gerenciamento de Endereços IP para Dispositivos Móveis

Índice

Visão Geral

O PGW-C aloca endereços IP para dispositivos UE (Equipamento do Usuário) quando eles estabelecem conexões PDN (Rede de Dados de Pacote). Esta é uma função crítica que permite que dispositivos móveis se comuniquem com redes externas.

Por que a Alocação de IP é Importante



Cada UE recebe um **endereço IP único** do PGW-C que:

- Identifica o dispositivo na rede
- Roteia o tráfego para/de o dispositivo
- Permite cobrança e aplicação de políticas
- Persiste durante a duração da conexão PDN

Versões de IP Suportadas

Versão de IP	Suporte	Descrição
IPv4	□ Completo	Endereços IPv4 padrão
IPv6	□ Completo	Endereços e prefixos IPv6
IPv4v6	□ Completo	Dual-stack (IPv4 e IPv6)

Conceitos de Alocação de IP

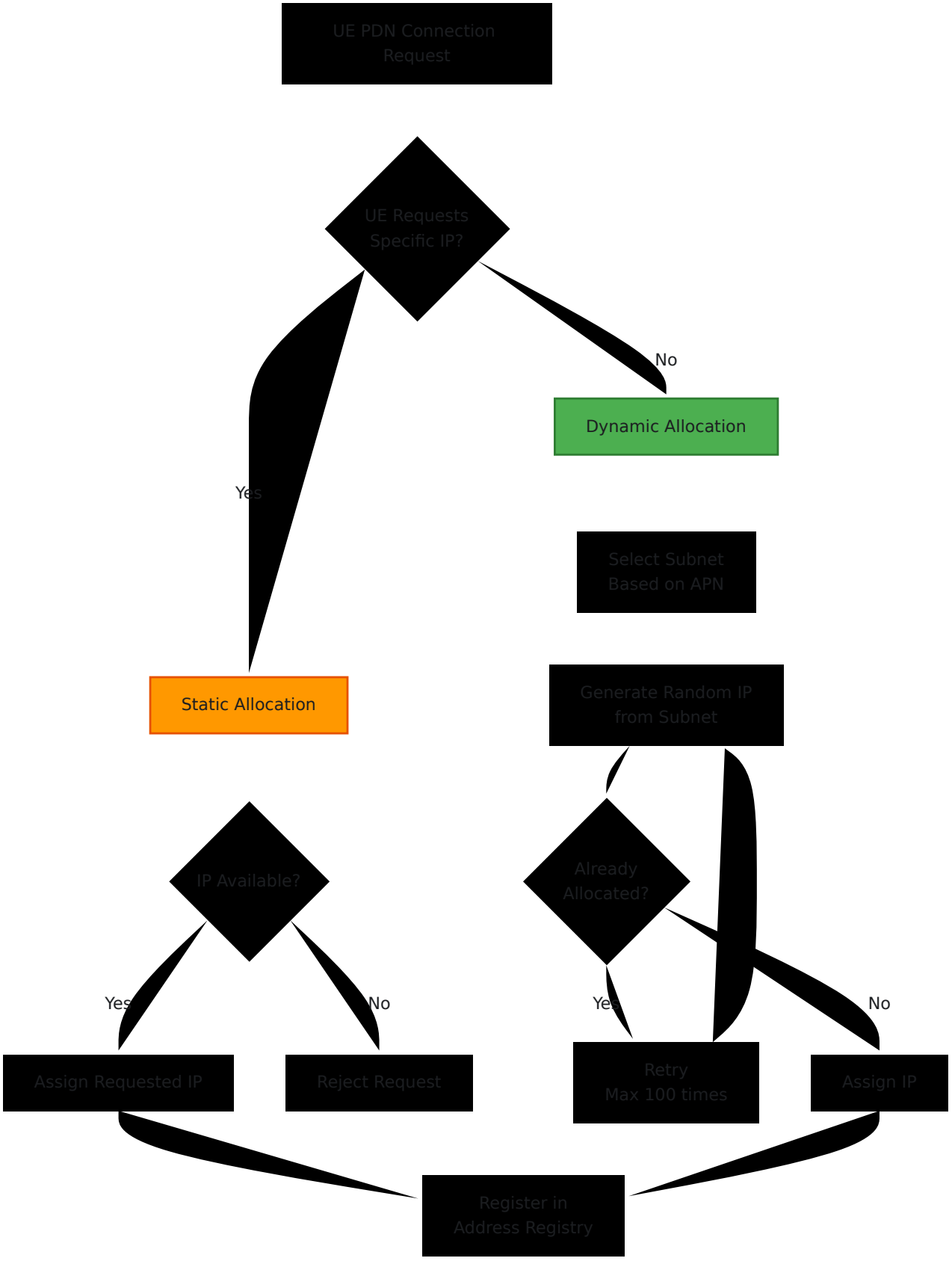
Tipo de PDN

Quando um UE solicita uma conexão PDN, ele especifica um **Tipo de PDN**:

Tipo de PDN	Descrição	Endereços Alocados
IPv4	Conexão apenas IPv4	Endereço IPv4 único
IPv6	Conexão apenas IPv6	Prefixo IPv6 (ex: /64)
IPv4v6	Conexão dual-stack	Endereço IPv4 e prefixo IPv6

Métodos de Alocação

O PGW-C suporta dois métodos de alocação de IP:



1. Alocação Dinâmica (Mais Comum):

- O PGW-C seleciona IP do pool configurado
- Seleção aleatória para evitar previsibilidade

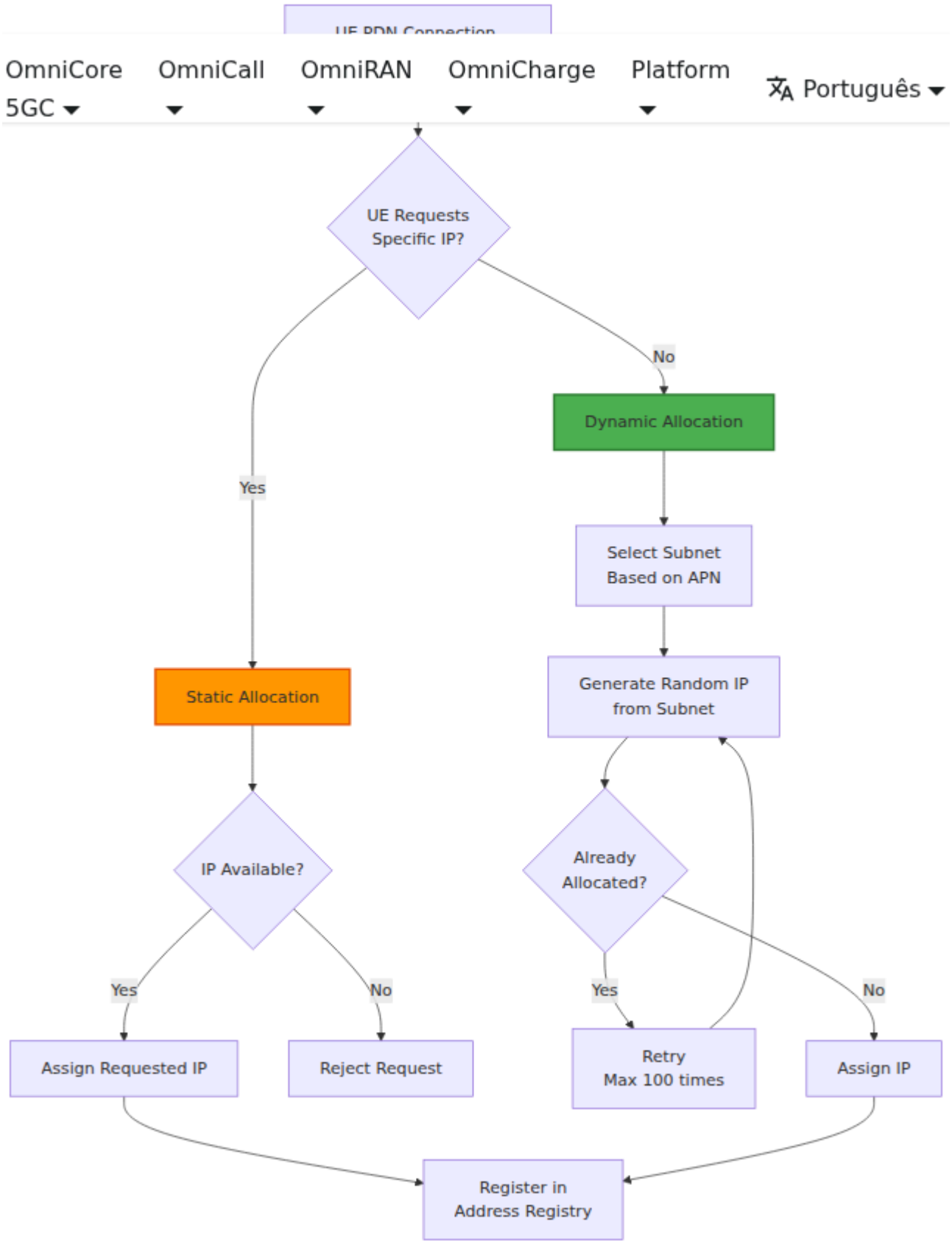
- Detecção de colisão garante exclusividade

2. Alocação Estática:

- UE solicita IP específico na mensagem GTP-C
- O PGW-C valida a disponibilidade
- Útil para dispositivos empresariais com IPs fixos

Seleção de Sub-rede Baseada em APN

Diferentes **APNs (Nomes de Ponto de Acesso)** podem usar diferentes pools de IP:



Benefícios:

- **Segregação de Tráfego** - Diferentes APNs roteiam para diferentes redes
- **Diferenciação de Políticas** - Aplicar políticas diferentes por APN

- **Planejamento de Capacidade** - Dimensionar pools com base no uso esperado
- **Cobrança** - Rastrear uso por tipo de serviço

Registro de Endereços

O **Registro de Endereços** rastreia IPs alocados:

Função	Descrição
Registro	Mapeia IP da UE → PID do Processo de Sessão
Consulta	Encontrar sessão pelo IP da UE
Desregistro	Liberar IP quando a sessão termina
Detecção de Colisão	Prevenir alocações duplicadas

Configuração

Configuração Básica

Edite `config/runtime.exs`:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # APN "internet" usa duas sub-redes
      "internet" => [
        "100.64.1.0/24",    # 254 IPs utilizáveis
        "100.64.2.0/24"     # 254 IPs utilizáveis
      ],

      # APN "ims" usa uma sub-rede
      "ims" => [
        "100.64.10.0/24"
      ],

      # Pool padrão para APNs desconhecidas
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Correspondência de Padrões Regex para APNs

Para cenários onde múltiplos APNs compartilham o mesmo pool de sub-rede, você pode usar **padrões regex** em vez de nomes exatos de APN. Isso é útil para correspondência de APN com curinga.

Regras de Padrão:

- Chaves começando com `^` são tratadas como padrões regex
- Chaves sem `^` são correspondidas exatamente (compatibilidade retroativa)
- Padrões são avaliados em ordem - o primeiro que corresponder vence
- Volta para `default` se nenhum padrão corresponder

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Regex: APNs começando com "ims" (ex: "ims", "ims.apn",
"ims.something.else")
      "^ims" => [
        "100.64.10.0/24"
      ],

      # Regex: APNs começando com "m2m." (ex: "m2m.test",
"m2m.prod")
      "^m2m\." => [
        "100.64.20.0/24"
      ],

      # Correspondência exata apenas - "enterprise.corp"
exatamente
      "enterprise.corp" => [
        "10.100.0.0/16"
      ],

      # Pool padrão para APNs não correspondidas
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Notas Importantes:

- Padrões regex usam a sintaxe padrão de regex do Elixir/Erlang
- As barras invertidas devem ser escapadas em strings do Elixir (use `\` para `\`)
- O `^` no início é necessário para indicar um padrão regex
- Correspondências exatas e padrões regex podem ser misturados na mesma configuração
- A ordem importa para padrões regex - coloque padrões mais específicos primeiro

Exemplos Comuns de Padrões:

Tipo de Padrão	Chave Regex	Correspondências
Começa com	`"^ims"`	`ims`, `ims.apn`, `ims.anything`
Termina com	`"^.*\.corp$"`	`foo.corp`, `bar.corp`
Contém	`"^.*test.*"`	`test`, `foo.test.bar`, `testing`
Exato (com pontos)	`"^internet\.apn$"`	`internet.apn` apenas

Exemplo de Correspondência de Sufixo:

Para corresponder APNs que terminam com um sufixo específico (como `.corp`), use `^.*\.suffix$`:

```
subnet_map: %{
  # Corresponder APNs que terminam com ".corp"
  "^.*\.corp$" => ["10.100.0.0/16"],

  # Corresponder APNs que terminam com ".iot"
  "^.*\.iot$" => ["10.200.0.0/16"],

  default: ["42.42.42.0/24"]
}
```

Exemplo de Correspondência de Padrão:

Solicitação de APN	Chave Correspondente	Pool Usado
`ims`	`^ims`	100.64.10.0/24
`ims.apn`	`^ims`	100.64.10.0/24
`ims.something.else`	`^ims`	100.64.10.0/24
`m2m.test`	`^m2m\.`	100.64.20.0/24
`m2m`	*default*	42.42.42.0/24
`enterprise.corp`	`enterprise.corp`	10.100.0.0/16
`foo.corp`	`^.*\.corp$`	10.100.0.0/16
`unknown.apn`	*default*	42.42.42.0/24

Notação de Sub-rede

Notação CIDR: `<rede>/<comprimento_do_prefixo>`

CIDR	IPs Utilizáveis	Faixa de Exemplo
/24	254	100.64.1.1 - 100.64.1.254
/23	510	100.64.0.1 - 100.64.1.254
/22	1022	100.64.0.1 - 100.64.3.254
/20	4094	100.64.0.1 - 100.64.15.254
/16	65534	100.64.0.1 - 100.64.255.254

Notas:

- O endereço de rede (ex: 100.64.1.0) não é alocado
- O endereço de broadcast (ex: 100.64.1.255) não é alocado
- O PGW-C aloca de `<rede> + 1` a `<broadcast> - 1`

Múltiplas Sub-redes por APN

Balanceamento de Carga Entre Sub-redes:

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24",
        "100.64.2.0/24",
        "100.64.3.0/24",
        "100.64.4.0/24"
      ]
    }
  }
```

Método de Seleção:

- O PGW-C seleciona aleatoriamente uma sub-rede da lista
- Fornece balanceamento de carga básico
- Cada sessão seleciona uma sub-rede independentemente

Benefícios:

- Distribuir carga entre múltiplas sub-redes
- Expansão de capacidade mais fácil (adicionar novas sub-redes)
- Flexibilidade para políticas de roteamento

Exemplo do Mundo Real

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # Acesso geral à internet
      "internet" => [
        "100.64.0.0/20"     # 4094 IPs para uso geral
      ],

      # IMS (Voz sobre LTE)
      "ims" => [
        "100.64.16.0/22"    # 1022 IPs para IMS
      ],

      # APN Empresarial
      "enterprise.corp" => [
        "10.100.0.0/16"     # 65534 IPs para empresas
      ],

      # Dispositivos IoT (baixa taxa de bits)
      "iot.m2m" => [
        "100.64.20.0/22"    # 1022 IPs para IoT
      ],

      # Fallback padrão
      default: [
        "42.42.42.0/24"     # 254 IPs para APNs desconhecidas
      ]
    }
  }
```

Configuração IPv6

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        # Pools IPv4
        "100.64.1.0/24"
      ],
      "internet.ipv6" => [
        # Pools IPv6 (delegação de prefixo)
        "2001:db8:1::/48"
      ],
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Delegação de Prefixo IPv6:

- O UE normalmente recebe um prefixo /64
- Permite que o UE atribua múltiplos IPs (ex: para compartilhamento de conexão)
- Exemplo: UE recebe `2001:db8:1:a::/64`

Configuração Dual-Stack (IPv4v6)

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24",        # Pool IPv4
        "2001:db8:1::/48"       # Pool IPv6 (será usado para
alocação IPv6)
      ]
    }
  }
```

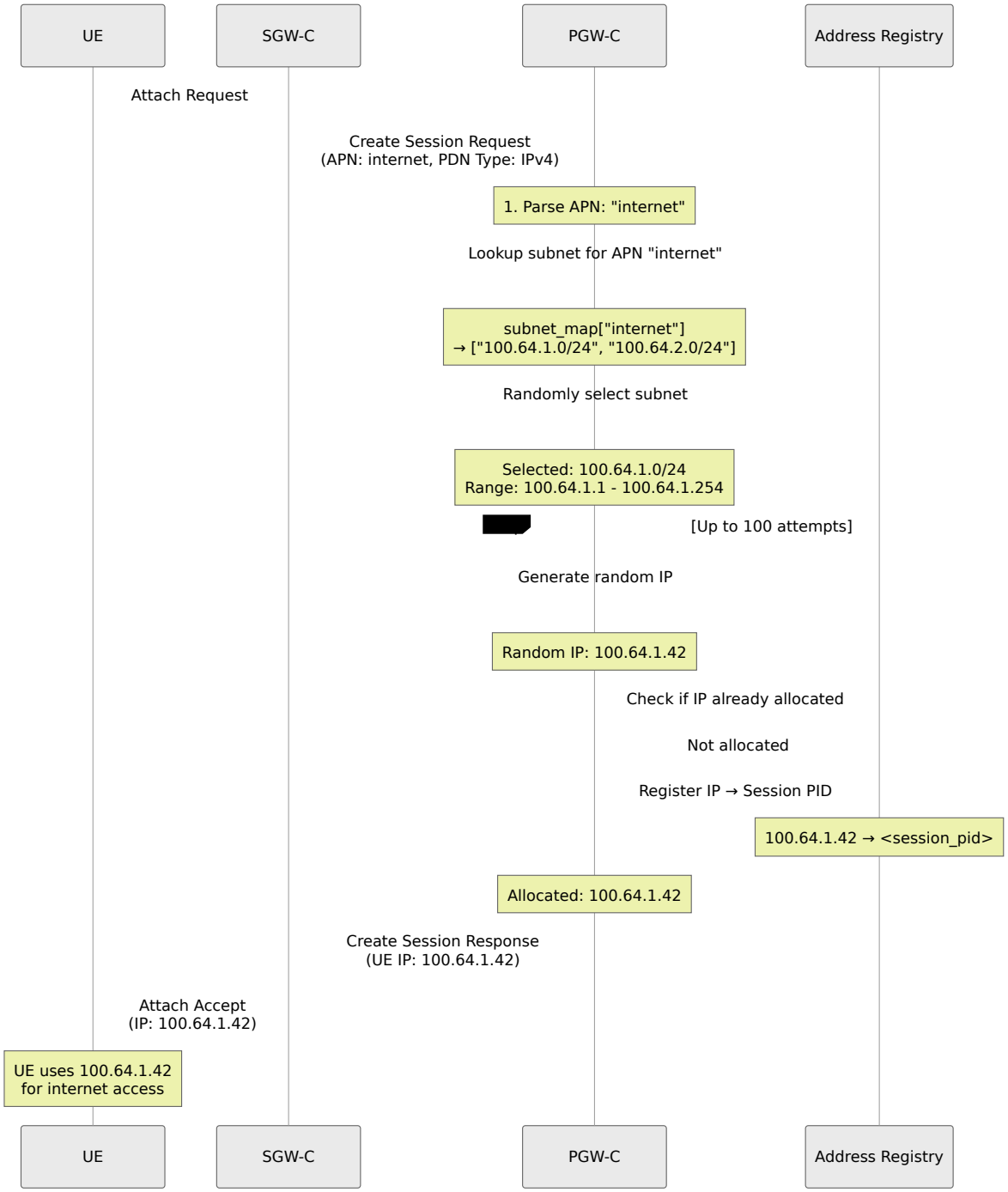
Alocação Dual-Stack:

- UE solicita Tipo de PDN: IPv4v6
- O PGW-C aloca tanto o endereço IPv4 quanto o prefixo IPv6
- Ambos os endereços ativos simultaneamente

Processo de Alocação

A alocação de IP ocorre durante a criação da sessão quando o PGW-C recebe uma Solicitação de Criação de Sessão via a interface S5/S8. Veja Interface S5/S8 para detalhes da mensagem GTP-C e Gerenciamento de Sessão para o ciclo de vida da sessão.

Passo a Passo: Alocação Dinâmica de IPv4



Como Funciona

Processo de Alocação Dinâmica:

1. **Consulta de Sub-rede:** O sistema recupera sub-redes configuradas para o APN solicitado

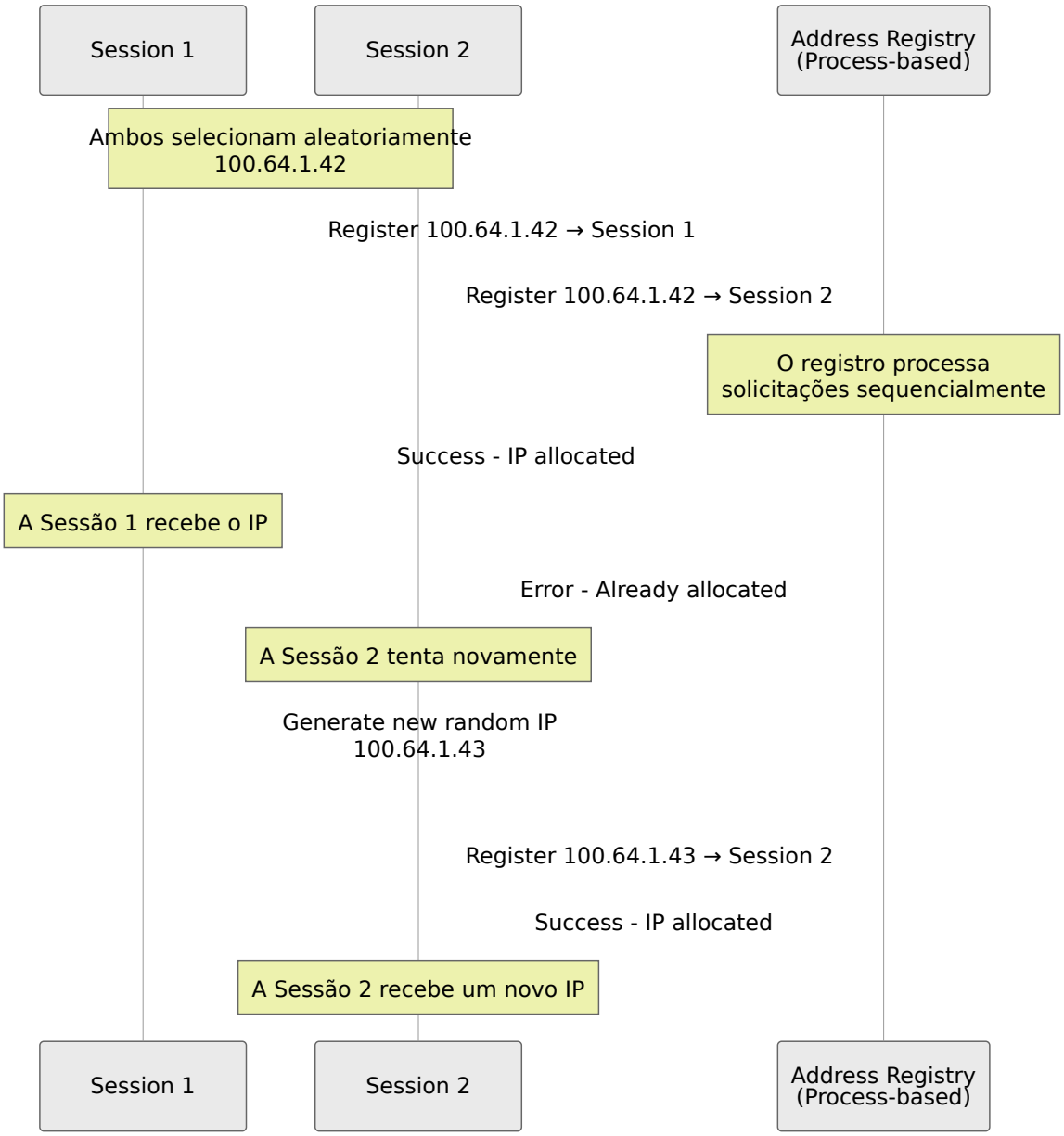
2. **Seleção Aleatória:** Uma sub-rede é selecionada aleatoriamente da lista disponível
3. **Geração de IP:** Um IP aleatório é gerado dentro da faixa da sub-rede
4. **Verificação de Exclusividade:** O sistema verifica se o IP não foi alocado
5. **Lógica de Retentativa:** Se uma colisão for detectada, retentativas até 100 vezes com um novo IP aleatório
6. **Registro:** Uma vez que um IP único é encontrado, ele é registrado na sessão

Pontos de Design Chave:

- **Máximo de 100 tentativas:** Previne loops infinitos quando o pool está quase esgotado
- **Seleção aleatória:** Evita padrões de atribuição de IP previsíveis para segurança
- **Operações atômicas:** O registro baseado em processo garante que não haja alocações duplicadas
- **Fallback para padrão:** Se o APN não for encontrado na configuração, usa o pool padrão

Manipulação de Colisões

Cenário: Duas sessões tentam alocar o mesmo IP simultaneamente



Como a Prevenção de Colisões Funciona:

- O registro processa solicitações uma a uma (serializado)
- Nenhuma condição de corrida é possível
- A primeira solicitação para registrar um IP tem sucesso
- Solicitações subsequentes para o mesmo IP são rejeitadas
- Sessões rejeitadas automaticamente tentam novamente com um novo IP aleatório

Fallback de Sub-rede Padrão

Cenário: UE solicita APN desconhecida

Exemplo de Configuração:

```
# Config
subnet_map: %{
  "internet" => ["100.64.1.0/24"],
  default: ["42.42.42.0/24"]
}
```

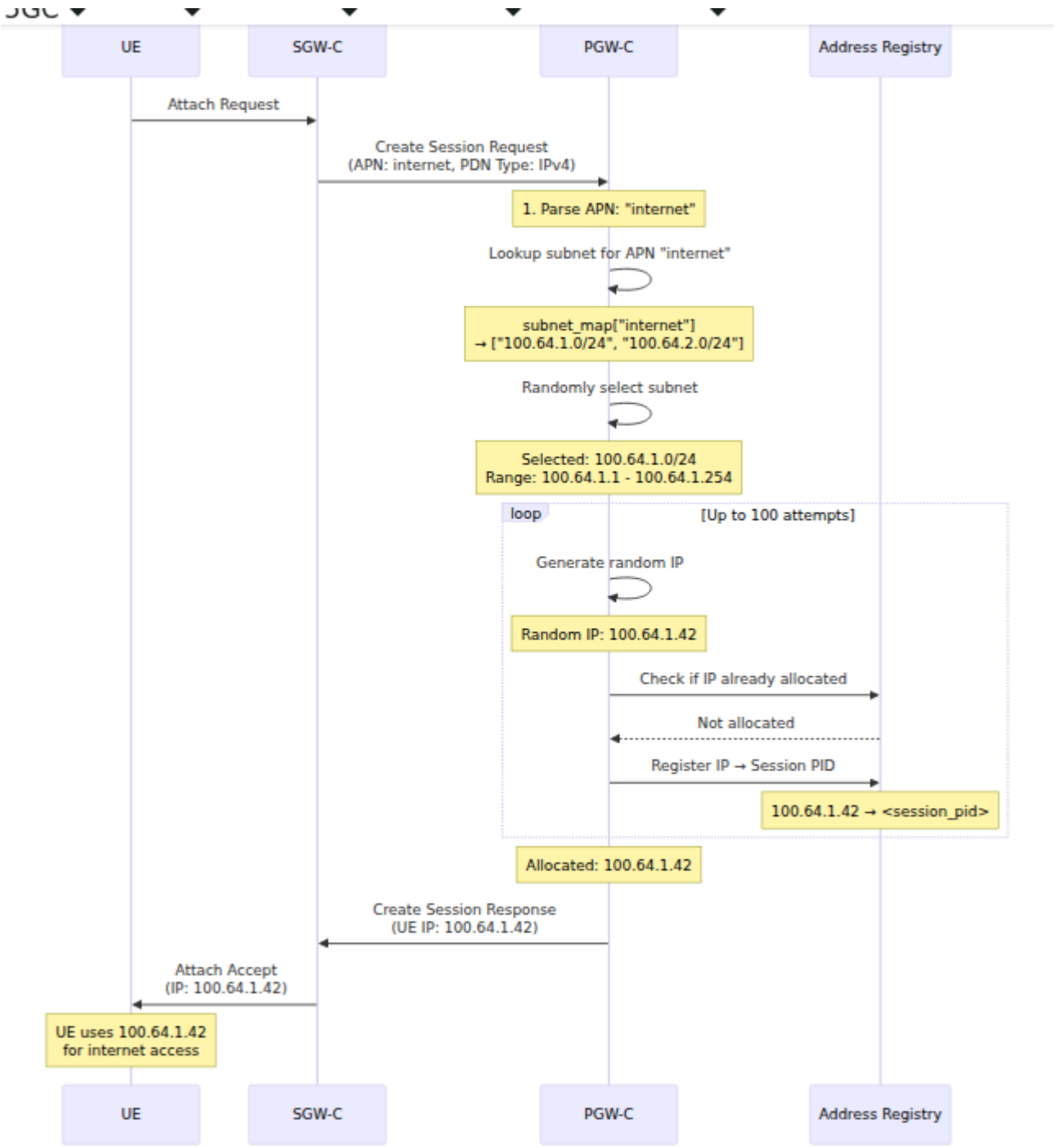
Comportamento:

- UE solicita APN: "unknown.apn"
- O sistema procura "unknown.apn" no subnet_map
- Não encontrado, então volta para o pool padrão
- Aloca IP do 42.42.42.0/24

Lógica de Fallback:

1. Primeiro, tenta encontrar o pool específico do APN na configuração
2. Se não encontrado, usa o pool `default`
3. Se nenhum padrão configurado, a alocação falha

Desalocação na Término da Sessão



Limpeza Automática:

- Quando o processo da sessão termina, o registro faz a limpeza
- O IP está imediatamente disponível para novas alocações
- Nenhuma intervenção manual é necessária

Tópicos Avançados

Esgotamento do Pool

Cenário: Todos os IPs no pool estão alocados

```
Pool: 100.64.1.0/24 (254 IPs utilizáveis)
Alocados: 254 IPs
Nova solicitação chega → Esgotamento
```

O que Acontece:

1. O PGW-C tenta 100 alocações aleatórias
2. Todas as tentativas encontram IP já alocado
3. Retorna: `{:error, :ue_ip_address_allocation_failed}`
4. A criação da sessão falha
5. O SGW-C recebe a resposta de erro

Prevenção:

```
# Monitorar utilização do pool
address_registry_count / total_pool_size > 0.8  # Alerta em 80%

# Expandir pool antes do esgotamento
"internet" => [
  "100.64.1.0/24",
  "100.64.2.0/24",  # Adicionar sub-rede adicional
  "100.64.3.0/24"
]
```

Alocação Estática de IP

Caso de Uso: Dispositivo empresarial precisa de IP fixo

Formato da Mensagem GTP-C:

```
Create Session Request
├── IMSI: 310260123456789
├── APN: enterprise.corp
├── PDN Address Allocation (IE)
│   └── PDN Type: IPv4
│   └── IPv4 Address: 10.100.0.50  ← UE solicita IP específico
```

Processamento do OmniPGW:

1. **Extrair IP Solicitado:** Analisar o IE de Alocação de Endereço PDN da solicitação
2. **Validar IP:** Verificar se o IP solicitado está no pool configurado para este APN
3. **Verificar Disponibilidade:** Confirmar que o IP não está alocado a outra sessão
4. **Alocar ou Rejeitar:**
   - Se disponível: Alocar o IP solicitado a esta sessão
   - Se indisponível: Rejeitar a sessão com o código de causa apropriado

Resultados Possíveis:

- **Sucesso:** UE recebe exatamente o endereço IP que solicitou
- **Falha (IP em uso):** Sessão rejeitada - IP já alocado
- **Falha (IP não no pool):** Sessão rejeitada - IP não está na faixa configurada

Delegação de Prefixo IPv6

UE solicita IPv6:

```
Create Session Request
├── PDN Type: IPv6
```

PGW-C aloca prefixo /64:

```
Prefixo Alocado: 2001:db8:1:a::/64

UE pode usar:
- 2001:db8:1:a::1
- 2001:db8:1:a::2
- ... (18 quintilhões de endereços)
```

Benefícios:

- UE pode atribuir múltiplos IPs (ex: compartilhamento de conexão)
- Suporta SLAAC (Configuração Automática de Endereço Sem Estado)
- Elimina a necessidade de NAT

Alocação Dual-Stack

UE solicita IPv4v6:

```
Create Session Request
├── PDN Type: IPv4v6
```

PGW-C aloca ambos:

```
IPv4: 100.64.1.42
IPv6: 2001:db8:1:a::/64
```

Manipulação de Tráfego:

- O tráfego IPv4 usa o endereço IPv4
- O tráfego IPv6 usa o prefixo IPv6
- Ambos ativos simultaneamente
- Túneis GTP separados (ou túnel dual-stack)

Endereços IP Privados vs. Públicos

Pools de IP Privados (RFC 1918):

```
# Não roteáveis na internet pública
subnet_map: %{
  "internet" => [
    "10.0.0.0/8",
    "172.16.0.0/12",
    "192.168.0.0/16"
  ]
}
```

Requer NAT no PGW-U para acessar a internet

Pools de IP Públicos:

```
# IPs públicos roteáveis (exemplo apenas)
subnet_map: %{
  "internet" => [
    "203.0.113.0/24"  # Bloco de IP público
  ]
}
```

Nenhum NAT necessário - roteamento direto para a internet

Recomendação:

- Use **IPs privados (RFC 6598)**: `100.64.0.0/10` (NAT de Grau de Operadora)
- Reserve IPs públicos apenas para serviços especiais

Monitoramento

UI Web - Gerenciamento de Pool de IP

O OmniPGW fornece uma interface web em tempo real para monitorar a alocação e utilização do pool de IP.

Acesso: `http://<omnipgw-ip>:<web-port>/ip_pools`

Recursos:

1. Visão Geral do Pool

- Total de IPs em todos os pools
- Endereços atualmente alocados
- IPs disponíveis restantes
- Porcentagem de utilização em tempo real

2. Status do Pool por APN Cada pool configurado exibe:

- **Nome do Pool** - Identificador do APN (ex: "default", "ims.something.else", "Internet")
- **Rótulo APN** - Distintivo do nome do APN configurado
- **Faixa de IP** - Notação CIDR mostrando a faixa da sub-rede
- **Utilização** - Indicador visual mostrando a porcentagem utilizada
- **Estatísticas de Alocação:**
  - Total: Número de IPs no pool
  - Alocados: IPs atualmente atribuídos
  - Disponíveis: IPs restantes para alocação

3. Atualizações em Tempo Real

- Atualização automática a cada 2 segundos
- Nenhum recarregamento de página necessário
- Rastreamento de utilização ao vivo

Casos de Uso:

- Verificação rápida de capacidade antes da manutenção
- Identificar pools se aproximando do esgotamento
- Verificar configuração do pool
- Monitorar padrões de alocação por APN

Métricas Chave

Contagem do Registro de Endereços:

```
# IPs atualmente alocados
address_registry_count

# Utilização do pool (requer cálculo)
address_registry_count / <total_pool_size> * 100
```

Exemplo:

```
Pool: 100.64.1.0/24 (254 IPs)
Alocados: 150 IPs
Utilização: 150 / 254 = 59%
```

Alertas

```yaml
# Alerta sobre alta utilização do pool
- alert: UEIPPoolUtilizationHigh
  expr: address_registry_count > 200  # Para pool /24
  for: 10m
  annotations:
    summary: "Utilização do pool de IP da UE acima de 80%"
    description: "Atual: {{ $value }} / 254 IPs alocados"

# Alerta sobre esgotamento do pool
- alert: UEIPPoolExhausted
  expr: address_registry_count >= 254  # Para pool /24
  for: 1m
  annotations:
    summary: "Pool de IP da UE esgotado - nenhum IP disponível"

# Alerta sobre falhas de alocação
- alert: UEIPAllocationFailures
  expr: rate(ue_ip_allocation_failures_total[5m]) > 0
  for: 5m
  annotations:
    summary: "Falhas de alocação de IP da UE ocorrendo"
```

Dashboard Grafana

Painel 1: Utilização do Pool de IP

```
# Gauge mostrando porcentagem
(address_registry_count / 254) * 100
```

Painel 2: IPs Alocados ao Longo do Tempo

```
# Série temporal
address_registry_count
```

Painel 3: Taxa de Alocação

```
# Taxa de novas alocações
rate(address_registry_count[5m])
```

Painel 4: Risco de Esgotamento do Pool

```
# Dias até o esgotamento (com base na taxa atual)
(254 - address_registry_count) / rate(address_registry_count[1h])
```

Solução de Problemas

Problema 1: Estabelecimento de Sessão Falha (Nenhum IP Disponível)

Sintomas:

- Resposta de Criação de Sessão: Causa "Solicitação rejeitada"
- Log: "Falha na alocação de endereço IP da UE"

Possíveis Causas:

1. **Pool Esgotado**

   ```
   # Verificar alocação atual
   curl http://<pgw_c_ip>:42069/metrics | grep
   address_registry_count
   ```

2. **Erro de Configuração**

```
# Verificar configuração da sub-rede
config :pgw_c,
  ue: %{
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24"  # Garantir CIDR válido
      ]
    }
  }
```

3. **Erro de Configuração de APN**

```
# Se APN não encontrado, volta para padrão
# Garantir que o pool padrão exista
subnet_map: %{
  default: ["42.42.42.0/24"]
}
```

Resolução:

- **Expandir pool:** Adicionar mais sub-redes
- **Limpar sessões obsoletas:** Reiniciar o PGW-C para liberar IPs vazados
- **Verificar configuração:** Checar `runtime.exs` por erros de digitação

Problema 2: Colisão de Endereço IP

Sintomas:

- Dois UEs recebem o mesmo IP (muito raro)
- Problemas de roteamento

Causa:

- Bug no Registro de Endereços (não deveria acontecer)

Debug:

```
# Verificar IPs duplicados nos logs
grep "already_registered" /var/log/pgw_c.log
```

Resolução:

- Deve se auto-corrigir (segunda sessão tenta novamente)
- Se persistente, relatar bug

Problema 3: Pool de IP Errado Usado

Sintomas:

- UE recebe IP de sub-rede inesperada
- APN "internet" recebe IP do pool "ims"

Causa:

- Configuração incorreta do subnet_map

Verificar:

```
# Verificar correspondência exata da string APN
subnet_map: %{
  "internet" => [...],    # Sensível a maiúsculas
  "Internet" => [...]     # APN diferente!
}
```

Resolução:

- Garantir que os nomes das APNs correspondam exatamente (sensível a maiúsculas)
- Usar pool padrão para captura

Problema 4: Falha na Alocação de IPv6

Sintomas:

- UE solicita IPv6, recebe erro

Possíveis Causas:

1. **Nenhum pool IPv6 configurado**

```
# Sub-redes IPv6 ausentes
subnet_map: %{
  "internet" => [
    "100.64.1.0/24"  # Apenas IPv4
  ]
}
```

2. **Prefixo IPv6 inválido**

```
# Prefixo muito pequeno (deve ser /48 ou maior)
"internet" => [
  "2001:db8::/128"  # Errado - sem espaço para alocação
]
```

Resolução:

```
# Adicionar pool IPv6
subnet_map: %{
  "internet" => [
    "100.64.1.0/24",
    "2001:db8:1::/48"  # Pool IPv6
  ]
}
```

Problema 5: Alta Utilização do Pool

Sintomas:

- Aproximando-se do esgotamento do pool
- `address_registry_count` se aproximando do máximo

Medidas Proativas:

1. **Adicionar Sub-redes:**

```
"internet" => [
  "100.64.1.0/24",   # Existente
  "100.64.2.0/24",   # Nova sub-rede (adiciona 254 IPs)
  "100.64.3.0/24"    # Nova sub-rede (adiciona 254 IPs)
]
```

2. **Usar Sub-redes Maiores:**

```
# Substituir /24 por /22
"internet" => [
  "100.64.0.0/22"  # 1022 IPs utilizáveis
]
```

3. **Limpeza de Sessões:**

   - Monitorar sessões obsoletas
   - Garantir o manuseio adequado da Solicitação de Exclusão de Sessão

---

Melhores Práticas

Planejamento de Capacidade

Calcular o tamanho do pool necessário:

```
Usuários simultâneos esperados: 10.000
Pico de concorrência: 30% (3.000 sessões simultâneas)
Buffer de crescimento: 50%
IPs necessários: 3.000 * 1.5 = 4.500 IPs

Sub-rede: /20 (4.094 IPs utilizáveis) - Muito pequeno
Sub-rede: /19 (8.190 IPs utilizáveis) - Suficiente
```

Seleção de Sub-rede

Recomendado:

- Usar `100.64.0.0/10` (RFC 6598 - NAT de Grau de Operadora)
- Fornece 4 milhões de IPs
- Reservado para NAT de provedor de serviços

Evitar:

- IPs públicos (caros, limitados)
- Faixas privadas comuns que conflitam com VPNs empresariais

Layout de Configuração

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # APN primário da internet - pool grande
      "internet" => [
        "100.64.0.0/18"  # 16.382 IPs
      ],

      # IMS - pool dedicado menor
      "ims" => [
        "100.64.64.0/22"  # 1.022 IPs
      ],

      # Empresarial - pool médio
      "enterprise.corp" => [
        "100.64.68.0/22"  # 1.022 IPs
      ],

      # IoT - pool grande para muitos dispositivos
      "iot.m2m" => [
        "100.64.72.0/20"  # 4.094 IPs
      ],

      # Padrão - fallback pequeno
      default: [
        "100.64.127.0/24"  # 254 IPs
      ]
    }
  }
```

Documentação Relacionada

Configuração

- **Guia de Configuração** - Configuração do pool de IP da UE, mapeamento de sub-rede APN

- **Configuração PCO** - DNS, P-CSCF, MTU entregues com endereço IP
- **Gerenciamento de Sessão** - Ciclo de vida da sessão, alocação de IP durante a configuração da PDN
- **Interface PFCP** - Atribuição de endereço UE via PFCP para UPF

Planejamento de Rede

- **Interface S5/S8** - Entrega de endereço IP via GTP-C
- **Interface Diameter Gx** - Controle de políticas para alocação de IP

Operações

- **Guia de Monitoramento** - Métricas de utilização do pool de IP, rastreamento de alocação
- **Formato de CDR de Dados** - Endereços IP da UE em CDRs para correlação de cobrança

---

Voltar ao Guia de Operações